



# **ONline 10BASE-T Security Module Installation and Operation Guide**

Document Number 17-00392-3  
Printed February 1996

Model Number: 5112M-TPLS

3Com Corporation  
118 Turnpike Road  
Southborough, MA 01772-1886  
U.S.A.  
(508) 460-8900  
FAX (508) 460-8950

## Federal Communications Commission Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you must correct the interference at your own expense.

## Canadian Emissions Requirements

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur la matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le Ministère des Communications.

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.

## VDE Class B Compliance

Hiermit wird bescheinigt, dass der 5112M-TPLS in Übereinstimmung mit den Bestimmungen der Vfg 243/1991 funktentspricht ist.

Der Deutschen Bundespost wurde das Inverkehrbringen dieses Gerätes angezeigt und die Berechtigung zur Überprüfung der Serie auf Einhaltung der Bestimmungen eingeräumt.

Einhaltung mit betreffenden Bestimmungen kommt darauf an, dass geschirmte Ausführungen gebraucht werden. Für die Beschaffung richtiger Ausführungen ist der Betreiber verantwortlich.

This is to certify that the 5112M-TPLS is shielded against radio interference in accordance with the provisions of Vfg 243/1991.

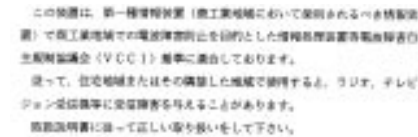
The German Postal Services have been advised that this equipment is being placed on the market and that they have been given the right to inspect the series for compliance with regulations.

Compliance with applicable regulations depends on the use of shielded cables. The user is responsible for procuring the appropriate cables.

## EN55022/CISPR22 Compliance

This equipment conforms to the Class A emissions limits for a digital device as defined by EN55022 (CISPR22).

## VCCI Class 1 Compliance



This equipment is in the 1st Class category (information equipment to be used in commercial or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment aimed at preventing radio interference in commercial or industrial areas.

Consequently, when the equipment is used in a residential area or in an adjacent area, radio interference may be caused to radio and TV receivers, and so on.

Read the instructions for correct handling.

## UK General Approval Statement

The ONcore Switching Hub, ONline System Concentrator, and ONsemble StackSystem Hub are manufactured to the International Safety Standard EN 60950 and are approved in the UK under the General Approval Number NS/G/12345/J/100003 for indirect connection to the public telecommunication network.

## Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by 3Com Corporation. 3Com Corporation assumes no responsibility for any errors that may appear in this document.

## Copyright Statement

© 1996, by 3Com Corporation. Printed in U.S.A. All rights reserved. 3Com is a registered trademark of 3Com Corporation. ONcore is a registered trademark of 3Com Corporation. The information contained herein is the exclusive and confidential property of 3Com Corporation. No part of this manual may be disclosed or reproduced in whole or in part without permission from 3Com Corporation.

## Trademarks

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all cases, these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

Artel, Chipcom, Ethermodem, Galactica, ONcore, ORnet, StarBridge, and TriChannel are registered trademarks of 3Com Corporation.

Chipcom OpenHub, G-Man, LANsentry, MultiProbe, ONdemand, ONline, ONsemble, PowerRing, SL2000, SL3000, SL4000, StackJack, StackSystem, and SwitchCentral are trademarks of 3Com Corporation.

The Chipcom Multichannel Architecture Communications System is registered under U.S. Patent Number 5,301,303.

XNS is a trademark and Ethernet is a registered trademark of Xerox Corporation.

DEC, DECnet, the Digital logo, DELNI, POLYCENTER, VAX, VT100, and VT220 are trademarks of Digital Equipment Corporation.

UNIX is a registered trademark in the U.S.A. and other countries licensed exclusively through X/Open Company, Ltd.

IBM is a registered trademark of International Business Machines.

3ComFacts, Ask 3Com, CardFacts, NetFacts, and CardBoard are service marks of 3Com Corporation.

3Com, LANplex, BoundaryRouting, LanScanner, LinkBuilder, NETBuilder, NETBuilderII, ParallelTasking, ViewBuilder, EtherDisk, EtherLink, EtherLink Plus, EtherLink II, TokenLink, TokenLink Plus, and TokenDisk are registered trademarks of 3Com Corporation.

3ComLaser Library, 3TECH, CacheCard, FDDILink, FMS, NetProbe, SmartAgent, Star-Tek, and Transcend are trademarks of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc.

3Com registered trademarks are registered in the United States, and may or may not be registered in other countries. Other brand and product names may be registered trademarks or trademarks of their respective holders.

## **Restricted Rights**

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Printed on recycled paper.



# Contents

## ***How to Use This Guide***

Audience . . . . .	xiii
Structure of This Guide . . . . .	xiv
Document Conventions . . . . .	xv
Related Documents . . . . .	xvi
3Com Documents . . . . .	xvii
Reference Documents . . . . .	xvii

## ***Chapter 1 – Introduction***

The ONline 10BASE-T Security Module . . . . .	1-1
Theory of Operation . . . . .	1-2
Application . . . . .	1-2
ONline Management . . . . .	1-3

## ***Chapter 2 – Designing and Expanding the Network***

Understanding the General Rules . . . . .	2-2
Basic Network Rules . . . . .	2-2
LAN Equivalence . . . . .	2-6
Fiber Backbone, Twisted Pair To-The-Desk . . . . .	2-7
Fiber Backbone, Twisted Pair To-The-Desk Example . . . . .	2-8
Twisted Pair Backbone, Twisted Pair To-The-Desk . . . . .	2-10
Patch Panels . . . . .	2-11
Redundant Links . . . . .	2-12

## ***Chapter 3 – Installing and Operating the Module***

Precautionary Procedures .....	3-2
Quick Installation Chart .....	3-2
Unpacking Procedures .....	3-4
Setting the Dip Switch .....	3-5
Installing the Module .....	3-8
Installing the Cable Tie-Wrap Kit .....	3-8
Installing the Module .....	3-11
Configuring the Module .....	3-13
Port Enable .....	3-14
Network Assignment .....	3-14
Port Redundancy .....	3-14
Link Integrity .....	3-15
Module Security .....	3-15
Autopartition Threshold .....	3-16
Saving Module Configurations .....	3-16
Reverting Module Configurations .....	3-16
Showing Module Configurations .....	3-17
Monitoring the Front Panel .....	3-18
LED and Network Verification .....	3-21

## ***Chapter 4 – Configuring Security Features***

Quick Reference for Configuring Security .....	4-2
Configuring Security Features .....	4-4
Eavesdropping Security .....	4-4
Intrusion Detection .....	4-5
Defining Port Security Type .....	4-6
Defining Port Action on Intrusion .....	4-7
Configuring Autolearning Mask .....	4-8
Enabling Ports .....	4-8
Configuring Autolearning .....	4-9
Defining a MAC Address Manually .....	4-11
Downloading the Autolearning Database .....	4-12
Configuring Security Mode .....	4-13
Saving Security Configurations .....	4-14
Reverting Security Configurations .....	4-14
Showing Security Configurations .....	4-14

Showing Port Configurations . . . . .	4-15
Showing Security Autolearn . . . . .	4-17
Showing Security Intruder List . . . . .	4-18
Clearing Security Configurations . . . . .	4-19
Clearing the MAC Address Table . . . . .	4-19
Clearing the Autolearning Database . . . . .	4-20
Clearing the Security Intruder List . . . . .	4-20
Using 3Com MIB Security Variables . . . . .	4-21
EMM Security SNMP Variables . . . . .	4-21
Using the Security Module SNMP Variables . . . . .	4-22

## ***Chapter 5 – Troubleshooting***

Troubleshooting . . . . .	5-1
Troubleshooting Using the Status LEDs . . . . .	5-2
Troubleshooting Using the Activity LEDs . . . . .	5-4
Technical Assistance . . . . .	5-5

## ***Appendix A – Specifications***

Electrical Specifications . . . . .	A-1
Environmental Specifications . . . . .	A-2
Mechanical Specifications . . . . .	A-2
General Specifications . . . . .	A-2
50-Pin Connector and Cable . . . . .	A-3
Twisted Pair Connectors and Cables . . . . .	A-6
Twisted Pair Connectors . . . . .	A-7
Twisted Pair Cables . . . . .	A-8

## ***Appendix B – Technical Support***

On-line Technical Support . . . . .	B-1
Email Technical Support . . . . .	B-2
World Wide Web Site . . . . .	B-2
Support from Your Network Supplier . . . . .	B-2
Support from 3Com . . . . .	B-3
Returning Products for Repair . . . . .	B-4
Accessing the 3Com MIB . . . . .	B-4
3Com Technical Publications . . . . .	B-5

## ***Index***



## ***Figures***

Figure 1-1.	ONline 10BASE-T Security Module Application . . . . .	1-3
Figure 2-1.	Sample Configuration Distance Calculation . . . . .	2-9
Figure 2-2.	Unshielded Twisted Pair Network . . . . .	2-11
Figure 2-3.	Redundant Twisted Pair Configuration . . . . .	2-12
Figure 3-1.	Security Module Dip Switch SW1 Location . . . . .	3-5
Figure 3-2.	Attaching the Tie-Wrap Bracket to the Module . . . . .	3-9
Figure 3-3.	Attaching Cables With 90° Connectors . . . . .	3-10
Figure 3-4.	Installing an ONline 10BASE-T Security Module . . . . .	3-11
Figure 3-5.	ONline 10BASE-T Security Module Cable Connection . . . . .	3-12
Figure 3-6.	Security Module Faceplate . . . . .	3-19
Figure 4-1.	Example of Eavesdropping Security . . . . .	4-5
Figure 4-2.	Example of Intrusion Detection . . . . .	4-6
Figure A-1.	50-Pin Cable Male and Female Connectors . . . . .	A-4
Figure A-2.	RJ-45 Connector Pinouts . . . . .	A-7



## ***Tables***

Table 2-1.	Seven Basic Network Rules . . . . .	2-3
Table 2-2.	LAN Product Equivalent Distances . . . . .	2-6
Table 2-3.	Maximum Link Distance on Twisted Pair . . . . .	2-10
Table 3-1.	Procedures for Completing Installation . . . . .	3-2
Table 3-2.	DIP Switch SW1 Network Selection Settings . . . . .	3-6
Table 3-3.	DIP Switch SW1 Security and Link Integrity Settings. . . . .	3-7
Table 3-4.	Interpretation of the Security Module LEDs . . . . .	3-20
Table 3-5.	Network Check Codes. . . . .	3-21
Table 4-1.	Quick Reference for Configuring the Security Module. . . . .	4-2
Table 5-1.	Troubleshooting Using the Port Status LEDs. . . . .	5-2
Table 5-2.	Troubleshooting Using the Activity LEDs . . . . .	5-4
Table A-1.	50-Pin Cable Pinouts and Port Assignments . . . . .	A-5



# *How to Use This Guide*

---

This guide tells you how to install and operate the 3Com ONline™ 10BASE-T Security Module (referred throughout this guide as the Security Module) for the ONline System Concentrator. A configuration section is provided to help you plan your network configuration. This guide also includes information on monitoring the module using an ONline network management module. An appendix explains cabling guidelines and options for this module.

---

## **Audience**

This guide is intended for the following people at your site:

- ☐ Network manager or administrator
- ☐ Hardware installer

---

## Structure of This Guide

This guide contains the following chapters:

***Chapter 1, Introduction*** – Introduces the principal features of the Security Module.

***Chapter 2, Designing and Expanding the Network*** – Explains examples of possible network configurations using the ONline System Concentrator and the Security Module.

***Chapter 3, Installing and Operating the Module*** – Provides illustrated procedures for installing the Security Module into the ONline System Concentrator. Also shows front panel LEDs and the DIP switch on the module.

***Chapter 4, Configuring Security Features*** – Describes the security features and provides the management commands to configure these features. Also provided are the commands to show and clear security configurations.

***Chapter 5, Troubleshooting*** – Provides help in isolating and correcting problems that may arise during the installation process and during normal operation.

***Appendix A, Specifications*** – Provides electrical, environmental, and mechanical specifications for the Security Module, plus information on the module's 50-pin Telco connector, RJ-45 connectors, and Twisted Pair cables.

***Appendix B, Technical Support*** – Lists the various methods for contacting the 3Com technical support organization and for accessing other product support services.





***Index***

---

## Document Conventions

The following document conventions are used in this manual:

Convention	Indicates	Example
Courier text	User input	In the Agent Information Form, enter <code>MIS</code> in the New Contact field.
	System output	After pressing the Apply button, the system displays the message <code>Transmitting data.</code>
Bold command string	Path names	Before you begin, read the <code>readme.txt</code> file located in <b><code>/usr/snm/agents</code></b> .
Italic text in braces	User-substituted identifiers	Use the following command to show port details: <code>SHOW PORT {slot.all} VERBOSE</code>
Capitalized text in plain brackets	Keyboard entry by the user	Type your password and press <code>[ENTER]</code> .
Italics	Text emphasis, document titles	Ensure that you press the Apply button <i>after</i> you add the new search parameters.

Convention	Indicates	Example
<b>Note:</b>	A <b>Note</b> . The information is important	<b>Note:</b> Use STP lobe cables for your system.
 <b>Caution:</b>	A <b>Caution</b> . A condition may damage software or hardware	 <b>Caution:</b> Do not put your installation diskettes on a magnetic surface. This may damage the diskettes.
 <b>Warning:</b>	A <b>Warning</b> . A condition may threaten personal safety	 <b>Warning:</b> Wear eye protection when performing these maintenance procedures.

## Related Documents

This section provides information on supporting documentation, including:

- ☐ 3Com Documents
- ☐ Reference Documents



## 3Com Documents

The following documents provide additional information on 3Com products:

*17-Slot ONline System Concentrator Installation and Operation Guide* – Explains how to install, operate, and manage the 3Com ONline 17-Slot System Concentrator (Models 5017C-LS and 5017C with load sharing).

*6-Slot ONline System Concentrator Installation and Operation Guide* – Explains how to install, operate, and manage the 3Com ONline 6-Slot System Concentrator.

*ONline Ethernet Management Module Installation and Operation Guide* – Describes how to install the ONline Ethernet Network Management Module in the ONline System Concentrator and explains the LEDs on the module faceplate. This guide also provides instructions for connecting a terminal to the module and describes the management commands necessary to perform management tasks on the concentrator and on remote devices.

*ONline Management Commands Guide* – Provides an alphabetized reference resource describing all ONline management commands.

For a complete list of 3Com documents, contact your 3Com representative.

## Reference Documents

The following documents supply related background information:

**Case, J., Fedor, M., Scoffstall, M., and J. Davin**, *The Simple Network Management Protocol*, RFC 1157, University of Tennessee at Knoxville, Performance Systems International and the MIT Laboratory for Computer Science, May 1990.

**Rose, M., and K. McCloghrie**, *Structure and Identification of Management Information for TCP/IP-based Internets*, RFC 1155, Performance Systems International and Hughes LAN Systems, May 1990.



# 1

## *Introduction*

---

This chapter describes the principle features of the ONline 10BASE-T Security Module.

---

### **The ONline 10BASE-T Security Module**

The ONline 10BASE-T Security Module is a 12-port IEEE 802.3 repeater module that complies with the 10BASE-T standard. The module is designed for use with the 3Com ONline System Concentrators using unshielded twisted pair wiring. The Security Module provides the following features and benefits:

- ❑ Provides jamming security for 12 10BASE-T ports
- ❑ Provides security from unauthorized transmissions
- ❑ Uses the 3Com ONguard™ technology to secure the network from eavesdropping and intrusions
- ❑ Supports up to 150 meter link distances on 22 gauge wire and up to 125 meters on 24 gauge wire (the meter distance on 26 gauge wire varies by cable type)
- ❑ Complies fully with the 10BASE-T signaling standard

- ❑ Features 'hot swap' capability so that you can install or remove the module without having to power down the concentrator

In addition, the Security Module allows you to disable Link Integrity, which allows the module to be connected to equipment that does not conform to the 10BASE-T standard.

Before installing the Security Module into the ONline System Concentrator, read the *ONline System Concentrator Installation and Operation Guide*.

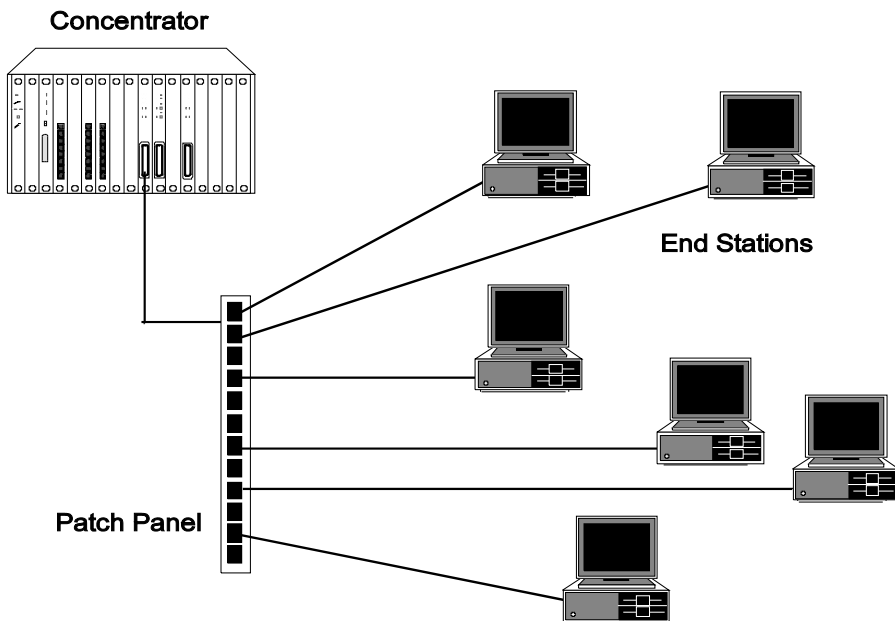
## Theory of Operation

The Security Module incorporates repeaters and twisted pair transceivers in its hardware:

- Repeaters restore phase and frequency. Repeated signals synchronize to the system clock and enter on the ONline concentrator's TriChannel™ backplane. Outgoing signals from the TriChannel backplane are sent directly to transceivers to be transmitted to twisted pair link segments.
- Transceivers receive and restore amplitude to incoming signals.

## Application

Attach the Security Module to a patch or punchdown block using bundled 25-pair or 12-leg hydra cables. This provides connections for the 12 twisted pair ports, as shown in Figure 1-1.



**Figure 1-1. ONline 10BASE-T Security Module Application**

## ONline Management

A *master* ONline Ethernet Management Module (EMM) at Version 4.0 is capable of managing the Security Module, including the Autolearning feature.

A master ONline Token Ring Management Module (TRMM) at Version 3.0 is capable of managing the Security Module *with the exception of the Autolearning Feature*. You must manually add MAC addresses to a port MAC address table in order for a TRMM to manage the security features of the Security Module. Refer to Chapter 4 for a description of the commands to add MAC addresses to a port MAC address table.



# 2 *Designing and Expanding the Network*

---

This chapter contains configuration information that will help you to design your network. Install all equipment using only approved cables for proper operation. Refer to Appendix A, Twisted Pair Connectors and Cables, for information on twisted pair connector and cable requirements.

This chapter includes five sections which describe how to configure your network using the ONline System Concentrator and the ONline 10BASE-T Security Module. These sections include:

- ❑ Understanding Network Configurations
- ❑ Fiber Backbone, Twisted Pair To-The-Desk
- ❑ Twisted Pair Backbone, Twisted Pair To-The-Desk
- ❑ Patch Panels
- ❑ Redundant Links

---

## Understanding the General Rules

As part of your network design, it is important to consider your network size. For instance, is the network (end-to-end) 100 meters, 1000 meters, 4000 meters, or more? What are your plans for expansion? Your answers play a role in how you configure your network. For example, once the network expands beyond a certain size, you need to add a bridge or other internetworking device.

This section describes general rules for configuring an Ethernet network using fiber as the backbone medium. It also provides rules to ensure that your network configuration conforms to distance limitations imposed by Ethernet and networking equipment.

This section includes:

- ❑ Basic Network Rules
- ❑ LAN Equivalence

## Basic Network Rules

This section outlines the basic network rules and 3Com's recommendations for these rules. For more hardware-specific information on the 10-Port module, refer to Appendix A.



Table 2-1 outlines the seven basic rules to keep in mind when you construct your network.

**Table 2-1. Seven Basic Network Rules**

Rule	Definition	Recommendations/Notes
1	If possible, use 10BASE-FB as the backbone medium.	Use 62.5 micron cable to conform with the IEEE 10BASE-F and upcoming ANSI FDDI standards.
		Use ST-type connectors.
2	Wire the backbone in a star topology to isolate faults.	Make sure to lay extra fiber cables. The extra cost is small and you will find you need them as your network grows.
		The star topology conforms to FDDI wiring as well -- just make sure to run at least two fiber strands to every backbone connection.
3	The maximum Fiber Ethernet network diameter is 4200 meters of fiber cable.	The 4200 meters is the maximum distance between any two transceivers on the network.
		The 4200 meters <i>does not include</i> the transceiver cable (that is, drop or patch cable) that connects a device with an external transceiver. Transceiver cables can extend up to 50 meters. Thus, total network diameter can be as much as 4300 meters ( $4200\text{ m} + 2 * 50\text{ m}$ ) between any two nodes.

**Table 2-1. Seven Basic Network Rules (Continued)**

Rule	Definition	Recommendations/Notes
4	Certain LAN devices on the network shrink the maximum Fiber Ethernet network diameter to less than 4200 meters.	Many LAN products delay the signal that goes through them. This is known as <i>equivalent distance</i> . Every microsecond delay reduces the maximum link distance. In fact, every microsecond delay shrinks the network diameter by approximately 200 meters of fiber cable. Table 2-2 lists the Equivalent Distances for other 3Com products.
5	Assume that one meter of coaxial or twisted pair is equal to one meter of fiber cable.	This is a conservative rule. For example, the actual equivalence is about 1.1 meters of coaxial for every meter of fiber. For simplicity, assume one meter.

**Table 2-1. Seven Basic Network Rules (Continued)**

Rule	Definition	Recommendations/Notes
6	The fiber link distances must not exceed the limits imposed by the optical power budget.	In general, on 62.5 micron cable, you can go up to 4000 meters point-to-point using the ONcore or ONline Fiber Modules. If you have poor quality cable or cross many patch panels, you may have to sacrifice some distance.
		Some older Ethernet fiber optic products are less powerful than ONcore Fiber Module optics. So when connecting to these products, remember that the least powerful device determines the maximum point-to-point distance.
7	When in doubt, use a bridge.	If you are not certain if you have exceeded allowable network distances, use a bridge to extend the network.

## LAN Equivalence

LAN equivalence is the sum of both the incoming and outgoing module port signals. Different modules, however, have different equivalent distances. Table 2-2 lists the LAN product equivalent distances..

***Table 2-2. LAN Product Equivalent Distances***

LAN Product	Equivalent Fiber Distance (meters)
ONline 10BASE-T Security Module (5112M-TPLS)	585
Incoming signal to TP port	420
Outgoing signal from TP port	165
ONline Ethernet 10BASE-FB Modules (5104M-FB, 5102M-FBP, 5104M-FBP)	190
Incoming signal to fiber port	140
Outgoing signal from fiber port	50
ONline Ethernet FOIRL Module (5104M-FL)	560
Incoming signal to fiber port	330
Outgoing signal from fiber port	230
ONline Ethernet 10BASE-T Module (5108M-TP)	585
Incoming signal to TP port	420
Outgoing signal from TP port	165
ONline Ethernet 50-Pin Module (5112M-TPL, 5112M-TPPL)	585
Incoming signal to TP port	420
Outgoing signal from TP port	165

**Table 2-2. LAN Product Equivalent Distances (Continued)**

LAN Product	Equivalent Fiber Distance (meters)
ONline Ethernet 24-Port Module (5124M-TPCL)	585
Incoming signal to TP port	420
Outgoing signal from TP port	165
ONline Ethernet Repeater Module (5102M-AUIF)	800
Incoming signal to AUI port	600
Outgoing signal from AUI port	200
ONline Ethernet BNC Module (5106M-BNC)	900
Incoming signal to BNC port	450
Outgoing signal from BNC port	450
ONline Ethernet Transceiver Module (5103M-AUIM)	0
3Com 10BASE-FB Star Coupler (9308S-FB)	180
ORnet Star Coupler (9314S)	180
IEEE Repeater	800

---

## Fiber Backbone, Twisted Pair To-The-Desk

When you configure a network with unshielded twisted pair cabling to-the-desk and fiber for the backbone, be aware of the following:

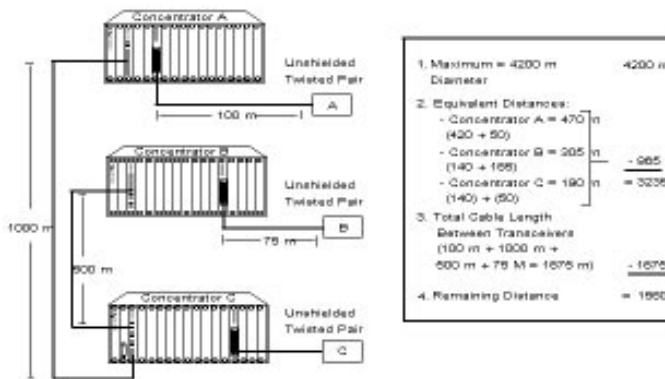
- ❑ You must add a bridge if you exceed four full repeaters. The four-repeater rule for Ethernet limits the number of 10BASE-T modules between any two transceivers. When traffic goes into a port on any repeater-based module and out the backplane, it counts as a 1/2 repeater. When the traffic goes into the module through one port and out another port on the same or a different module, it counts as one full repeater. Therefore, you must add a bridge if the path from one transceiver to another exceeds the four-repeater rule.
- ❑ The equivalent fiber distance for the ONline Ethernet Fiber Modules (see Rule 4) is:
  - 140 meters for signals that externally enter a Fiber Module port
  - 50 meters for signals that internally enter a Fiber Module through the ONline Concentrator backplane
- ❑ The equivalent fiber distance for the Security Module (see Rule 4) is:
  - 420 meters for signals that externally enter a Security Module
  - 165 meters for signals that internally enter a Security Module through the ONline System Concentrator backplane

For every pair of Security Modules that a signal goes through, deduct a fiber equivalent distance of 585 meters ( $420\text{ m} + 165\text{ m} = 585\text{ m}$ ) from the overall allowable network diameter. This is also true if a signal makes a roundtrip through a single Security Module (enters the Security Module through one port and exits another port of the same Security Module). This counts as 585 meters of fiber equivalent distance, *and* as a full repeater.

### **Fiber Backbone, Twisted Pair To-The-Desk Example**

In the sample configuration shown in Figure 2-1, we determine if the transceivers are within legal Ethernet limits. 22-gauge unshielded twisted pair cable is used to connect 10BASE-T Transceivers to the Security Modules in the concentrators.

Using the sample configuration below, identify the two transceivers that are likely to be the greatest fiber equivalent distance apart. In this case, they are 10BASE-T Transceivers A and B.



**Figure 2-1. Sample Configuration Distance Calculation**

To determine if your network configuration is legal:

1. Use 4.2 km (4200 m) since this is the maximum network diameter for a pure fiber network (see Rule 3).
2. Calculate the equivalent distances for each concentrator, and subtract the totals from 4200 (refer to Figure 2-1 for details).
3. Subtract all cable lengths between the two transceivers. If the result is greater than zero, the configuration is within legal Ethernet limits (see Rule 5).

For the configuration shown in Figure 2-1 to work, ensure the fiber equivalent distance between transceiver A and transceiver B is less than 4200 meters. As the calculation illustrates, 1560 meters remain for expansion in this configuration.

Do not exceed the distances as defined in Table 2-2 for the link from a Security Module to a 10BASE-T Transceiver.

**Table 2-3. Maximum Link Distance on Twisted Pair**

Cable Gauge	Supports Link Distances Up To:
Unshielded Twisted Pair: 10BASE-T	Normal Squelch
22 (.6 mm)	100 m
24 (.5 mm)	100 m

---

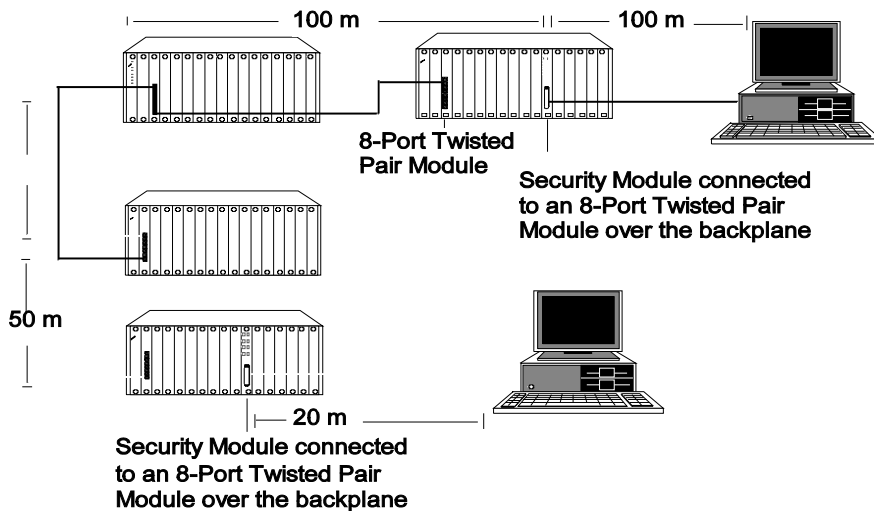
## Twisted Pair Backbone, Twisted Pair To-The-Desk

In constructing a twisted pair backbone, one additional configuration rule must be considered. Ensure there are no more than eight Security Modules in the path between any two transceivers due to Ethernet's four-repeater rule. This is because each Security Module counts as a 1/2 repeater *unless* the signal goes in one port and out another port of the same module, in which case the module counts as a full repeater.

If you have more than eight Security Modules serially connected, add a bridge. Each bridge creates a subnetwork. Each subnetwork can have its own 420 meter network diameter.

The configuration in Figure 2-2 illustrates a possible unshielded twisted pair network using 22 gauge cable.





**Figure 2-2. Unshielded Twisted Pair Network**

While there is no fiber in the configuration in Figure 2-2, you can calculate the fiber equivalent distance as follows:

Total link distance:  $100\text{ m} + 100\text{ m} + 100\text{ m} + 50\text{ m} + 20\text{ m} = 370\text{ m}$

Total equivalent distance of the Security Modules:  $(4 * 420\text{ m}) + (4 * 165\text{ m}) =$

$2340\text{ m}$  (signal externally enters four Twisted Pair Modules:  $4 * 420\text{ m}$ )

(signal enters four Twisted Pair Modules from the backplane:  $4 * 165\text{ m}$ )

Total equivalent distance:  $370\text{ m} + 2340\text{ m} = 2710\text{ m}$

Since the total equivalent distance (2710 m) is less than 4200 meters, this example is a legitimate configuration.

## Patch Panels

Patch panels weaken signals that pass through them, thereby reducing achievable link distances. 3Com assumes the use of one patch panel in the 100 meter link distance calculations specified in this manual. However, each additional patch panel in the link reduces the 100 meter link distance by approximately 10 meters.

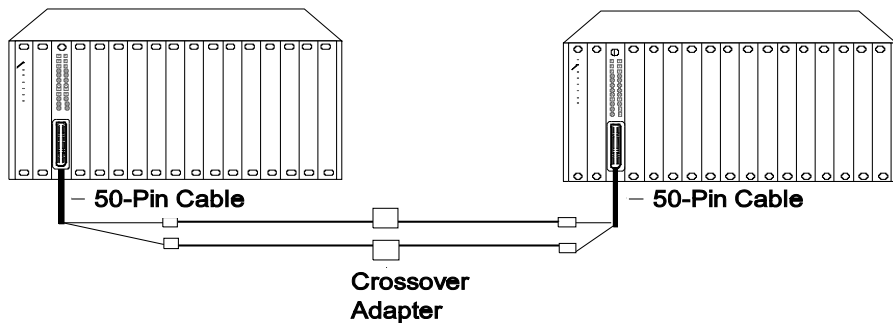
In the example shown in Figure 2-2, if two patch panels were used between the top right PC and the top right concentrator, you would have to shorten the link distance of 100 meters to 90 meters. This is because the maximum allowable link distance on 22 gauge wire using 10BASE-T signaling with two intervening patch panels is 100 meters minus approximately 10 meters.

Note that a patch panel installed between the bottom right PC and the bottom left concentrator would not affect the link because it is only 20 meters away.

---

## Redundant Links

You can implement twisted pair link redundancy between ONline System Concentrators using network management. Figure 2-3 shows an example of a redundant configuration between concentrators using Security Modules.



**Figure 2-3. Redundant Twisted Pair Configuration**

To set link redundancy between two Security Modules:

1. Connect two links to two ports on the 50-Pin Telco cables between the modules. Use a crossover adapter between each link because the links are designed to be connected to a station's port, not to other concentrator ports.
2. Use the SET PORT {slot.port} MODE REDUNDANT {slot.port} network management command to specify which port is the primary link and which is the backup link.

**Note:** If the Security Modules are powered down, and powered up without a 3Com network management module present, a network loop could occur. To prevent a potential network failure, set the DIP switch for the backup port to disable.

3. Once link redundancy is configured, a switchover occurs under two conditions: a link failure or a port partition. The switchover occurs when the primary link fails.
4. Once the switchover occurs and the backup link becomes operational, a switchover back to the primary link happens automatically once the problem is resolved.

**Note:** If you use a Security Module port as a backbone connection ensure that Security Mode is disabled for the port or it will experience security intrusion attempts.

Refer to the appropriate network management module installation and operation guide for information on setting redundancy between Security Module ports.



# 3 *Installing and Operating the Module*

---

This chapter describes the installation procedures and initial setup commands for the ONline 10BASE-T Security Module. For your convenience, a quick installation chart is included.

**Note:** Read the precautionary procedures before unpacking the module.

The remainder of this chapter describes:

- ❑ Setting the DIP Switch
- ❑ Installing the Module
- ❑ Configuring the Module
- ❑ Showing Module Configurations
- ❑ Monitoring the Front Panel

---

## Precautionary Procedures

Electrostatic discharge (ESD) can damage static-sensitive devices on circuit boards. Follow these precautions when you handle the Security Module:

- ❑ Do not remove the board from its anti-static shielding bag until you are ready to inspect it.
- ❑ Handle the board by the faceplate.

Use proper grounding techniques when you install the Security Module. These techniques include using a foot strap and grounded mat or wearing a grounded static discharge wrist strap. An alternate method is to touch the grounded rack or other source of ground just before you handle the module.

---

## Quick Installation Chart

Table 3-1 outlines the steps necessary to complete the installation of your module. If you are familiar with these instructions, you may want to use this table as a checklist; otherwise, consult the remainder of this chapter.

***Table 3-1. Procedures for Completing Installation***

Step	Procedure	Reference
1.	Verify that your network complies with the basic rules for network design.	<i>Chapter 2/Designing &amp; Expanding the Network</i>
2.	Unpack the module.	<i>Unpacking Procedures</i>
3.	If you do not have a management module installed in the concentrator, set the DIP switch settings to your specifications.	<i>Setting the DIP Switch</i>

**Table 3-1. Procedures for Completing Installation (Continued)**

Step	Procedure	Reference
4.	Install the module into a blank slot in the concentrator and tighten the faceplate screws.	<i>Installing the Module</i>
5.	Establish connections from the Security Module to devices or a 10BASE-T transceiver using the appropriate connectors and cabling.	<i>Installing the Module</i>
6.	If you have a management module installed in the concentrator, configure the module using the management commands.	<i>Configuring the Module</i>
7.	Verify LED status for normal operation. <b>Note:</b> To resolve potential problems, consult the troubleshooting techniques in Chapter 5.	<i>LED and Network Verification</i>

---

## Unpacking Procedures

To unpack your Security Module:

1. Verify that the Security Module is the correct module by matching the model number listed on the side of the shipping carton to the model number you ordered.

Note that the product model number printed on the shipping box differs from the model number on the product. The model number on the shipping box contains the prefix '3C9'.

If the module appears to be damaged, return it to the anti-static shielding bag, repack it in the shipping carton, and contact your local 3Com supplier.

2. Remove the Security Module, in its anti-static bag, from the shipping carton.
3. Remove the module from the anti-static shielding bag and inspect it for damage. Save the package of screws in the carton; you will need them when you attach a cable to the module. Always handle the Security Module by the faceplate, being careful not to touch the components.

Keep the shipping carton and anti-static shielding bag in which your module was shipped in case you want to repackage the module for storage or shipment. Record the serial number of your Security Module. A log for information specific to your modules is provided under the Slot Usage Chart in Appendix B of the *ONline System Concentrator Installation and Operation Guide*.



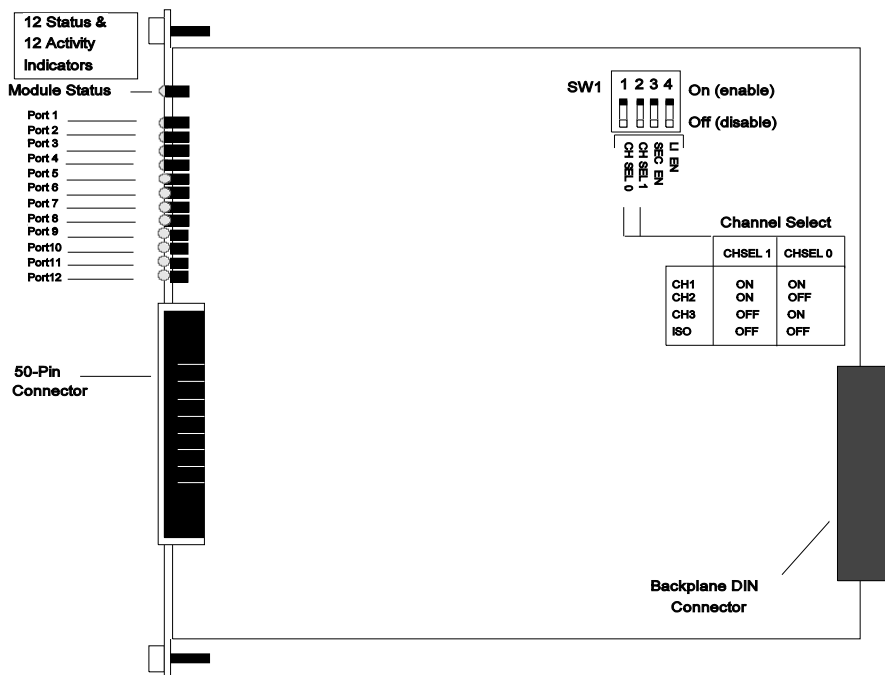
---

## Setting the Dip Switch

The Security Module has one 4-switch DIP switch (SW1) located on the module. The functions of the DIP switch settings on the Security Module are ignored if a management module is already installed in the concentrator. For this reason, use management commands, rather than the DIP switch, to configure the module.

If a management module is installed in the concentrator, you may skip this section and proceed to the Installing the Module section later in this chapter.

Figure 3-1 shows the location and default settings of the DIP switch.



**Figure 3-1. Security Module Dip Switch SW1 Location**

Network selection switches 1 and 2 enable you to select a channel for the module. Switches 1 and 2 are factory set to On. Therefore, the Security Module is initially configured to network 1. To reconfigure the module to a different network, refer to the information in .

**Table 3-2. DIP Switch SW1 Network Selection Settings**

	Switch 1	Switch 2	Network Selection
Switch Settings	On	On	1 (default)
	Off	On	2
	On	Off	3
	Off	Off	Isolated (module operates independently of the three backplane networks)

Switch 3 (Security) allows you to enable or disable Security mode and enable or disable port mode for all 12 ports on the Security Module. Switch 3 is configured to affect both Security mode and the port mode setting in order to protect your ports in the event the management module fails.

When the Security switch is set to *enabled*, port mode is set to *disabled*. Conversely, when the Security switch is set to *disabled*, port mode is set to *enabled*.

This dual purpose setting provides maximum security for all ports on the Security Module and also provides you with the flexibility of using the ports as non-secure ports in the event the management module fails. Without management, you may elect to have traffic continue to pass through the non-secure ports. However, your environment may require secure ports at all times. In this situation, you would choose to disable the ports rather than keep them enabled in a non-secure environment.

Switch 4 (Link Integrity) allows you to enable or disable Link Integrity. Table 3-3 lists the functions and default settings for switches 3 and 4.

**Table 3-3. DIP Switch SW1 Security and Link Integrity Settings**

Switch	Function	Factory Default	Switch Setting Off On	
3 (Security)	Enable or disable security <i>and</i> enable or disable port mode for all 12 ports	enable	Security disable/ Port enable	Security enable/ Port disable
4 (Link Integrity)	Enable or disable link integrity for all 12 ports.	enable	disable	enable

The complete definition of each dip switch function is contained in the Configuring the Module section later in this chapter.

---

## Installing the Module

You do not need to power down the ONline System Concentrator to install the Security Module. You can insert the module while the concentrator is operating (this is called a *hot swap*).

This section describes:

- ☐ Installing the Cable Tie-Wrap Kit
- ☐ Installing the Module

### Installing the Cable Tie-Wrap Kit

A cable tie-wrap kit is included with the Security Module. If you use a cable connector other than a 180° cable connector (for example, a 90° cable connector), you must secure the cable to the module connector using the tie-wrap kit. 3Com recommends using a 180° cable connector with the Security Module.

If you are using a 180° cable connector with the Security Module, skip this procedure and proceed to the next section, Installing the Module.

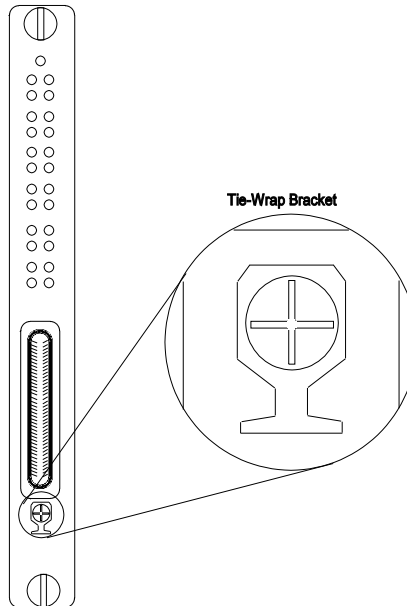
**Note:** Perform the tie-wrap kit installation procedure prior to installing the module into a 3Com ONline System Concentrator.

The tie-wrap kit contains:

- ☐ Kit card containing kit part number
- ☐ 1 Phillips-head screw
- ☐ 1 Tie-wrap bracket
- ☐ 3 Tie-wraps

To install the tie-wrap kit:

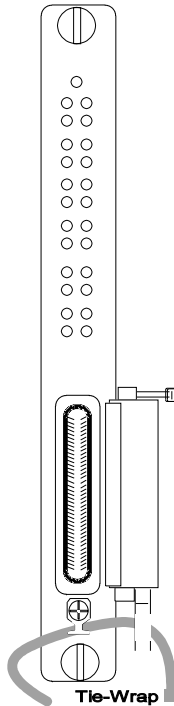
1. Remove the hex nut from the bottom of the connector located on the module faceplate.
2. Using the Phillips-head screw provided in the tie-wrap kit, attach the tie-wrap bracket to the module (Figure 3-2).



**Figure 3-2. Attaching the Tie-Wrap Bracket to the Module**

3. Insert the tie-wrap through the opening on the tie-wrap bracket.

4. Connect the 90° cable connector to the module connector using a tie-wrap to secure the cable connector to the module (Figure 3-3).



**Figure 3-3. Attaching Cables With 90° Connectors**

5. Wrap the tie-wrap around the cable connector to secure the cable connector to the module connector.

**Caution:** Do not fasten the tie-wrap around the module ejectors.

## Installing the Module

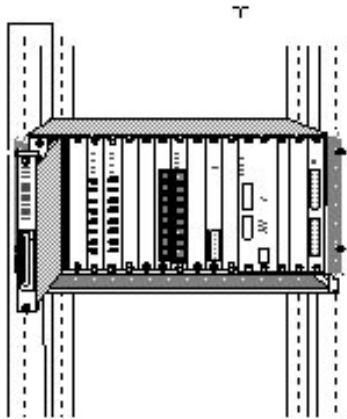
To install the Security Module:

1. If you do not have a management module installed in the concentrator, make sure you set the DIP switches properly on the board, if different than the default settings.

A management module is required to configure the security features of the Security Module. Without management, the Security Module functions as a non-secure 10BASE-T module.

2. Locate an open slot in the concentrator. Remove the blank panel on the concentrator to expose a slot for the module.

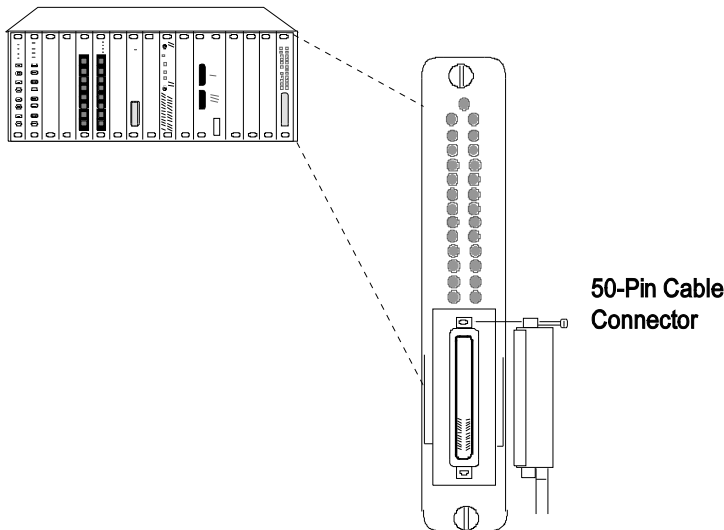
Insert the module into the board guides at the top and bottom of the slot and slide it into the concentrator by firmly pressing the top and bottom of the faceplate. Make sure the connector is well-seated into the backplane of the concentrator. Figure 3-4 shows the installation of the module.



**Figure 3-4. Installing an ONLine 10BASE-T Security Module**

3. Fasten the spring-loaded screws on the front of the Security Module faceplate to the concentrator with your fingers (do not overtighten).

4. Remove the long screw (if present) from the 50-pin cable. Discard this screw.
5. Remove the two cable-fastening screws from the Security Module shipping carton.
6. Attach the 50-pin cable connector to the 50-pin connector on the front of the module.
7. Install the two screws in the top and bottom screw holes of the 50-pin cable connector to secure the cable to the module connector as shown in Figure 3-5. (Only one of the cable-fastening screws may be installed depending on the angle of the 50-pin cable connector.)



**Figure 3-5. ONline 10BASE-T Security Module Cable Connection**

8. Attach the other end of the cable to a 10BASE-T Transceiver or a 10BASE-T Adapter Card.



The 50-pin Telco-type connector connects to 12 10BASE-T-compliant ports using a 12-leg hydra cable. This module can be attached using the 12-leg hydra cable to a patch panel or punch-down block, which provides connections for the 12 twisted pair ports.

The next section describes the features you can set for the Security Module.

---

## Configuring the Module

The ONline management modules (EMM, TRMM, and FMM) provide management capabilities for the ONline System Concentrator and its modules. If a management module is already installed, the DIP switch settings on the Security Module are ignored. For this reason, 3Com recommends that you use management commands, rather than the DIP switches, to configure the module and the ports.

When you first install the module and network management is present:

1. The network defaults to isolated mode and the ports are automatically disabled so that unapproved users cannot be added.
2. You must enable the ports you wish to use and set the module to the appropriate network through the management commands.

The following sections describe the management commands to set the above features. Refer to the appropriate ONline management module installation and operation guide and the *ONline Management Commands Guide* for additional information on available network management features.

## Port Enable

You can enable or disable use of the 12 ports on the Security Module. When a port is enabled, it can transmit and receive data onto the network to which the module is assigned. 3Com recommends that you disable all unused ports on the Security Module to prevent network tampering.

Enter the following management command to enable all the ports on the module in slot 3.

```
ONline> set port 3.all mode enable [ENTER]
```

## Network Assignment

The Security Module is equipped with the technology to work with the ONline System Concentrator's unique TriChannel™ architecture. This feature allows you to assign the module to any of three networks or isolated on the ONline System Concentrator backplane. Refer to the *ONline System Concentrator Installation and Operation Guide*, Chapter 1, for a discussion of the ONline TriChannel architecture.

Enter the following management command to assign the Security Module in slot 3 to Ethernet network 1.

```
ONline> set module 3 network ethernet_1 [ENTER]
```

## Port Redundancy

ONline network management allows you to set redundancy between ports. Enter the following management command to set redundancy between ports on the Ethernet module in slot 5.

```
ONline> set port 5.1 mode redundant 5.2 [ENTER]
```

Use the MODE NON\_REDUNDANT option to turn off redundancy between ports. Recommended redundancy configurations are shown in Chapter 2, Designing and Expanding the network.

If you set up redundancy between a secure port and a non-secure port (whether on a Security Module port or other module port), a warning message is displayed to terminal management. The warning informs you that this configuration has the potential to automatically cause a change in security when the primary port fails and the secondary port becomes activated.

## Link Integrity

In general, enable Link Integrity for the Security Module to conform to the 10BASE-T standard. Disable Link Integrity to connect to older equipment that does not conform to the 10BASE-T standard.

Enable Link integrity at both ends or disable Link Integrity at both ends of the connection. If one end of the connection is different, the module with Link Integrity enabled reports a Link Integrity error.

If you enable a port and disable Link Integrity, the Status LED for that port is on for 10 seconds and blinks off for 400 msec to indicate that Link Integrity is disabled.

Enter the following management command to enable Link Integrity for all ports on the Ethernet module in slot 5.

```
ONline> set port 5.all link_integrity enable [ENTER]
```

## Module Security

The Module Security DIP switch allows you to enable or disable security for the module. 3Com recommends that you leave this switch in its factory default setting (Off). This setting ensures that in the unlikely event of a concurrent failure of both the master management module and concentrator power, the Security Module ports will power up with ports disabled in a concentrator without network management.

**Note:** When the Security switch is set to *enabled*, port mode is set to *disabled*. Conversely, when the Security switch is set to *disabled*, port mode is set to *enabled*.

Use the following command to enable security for all of the ports on the Security Module in slot 3.

```
ONline> set security port 3.all mode enable [ENTER]
```

## Autopartition Threshold

Autopartition threshold tells network management the number of collisions to allow before automatically partitioning a port. The options are 31, 63, 127, and 255. The factory default is 63. The 10BASE-T specification lists a minimum of 31 collisions prior to partition, but 31 collisions can cause ports to partition more frequently than necessary.

The additional options (127 and 255) are for debugging purposes, and therefore not recommended for use in live networks.

Enter the following command to define 127 collisions for the module in slot 3.

```
ONline> set module 3 autopartition_threshold 127_coll [ENTER]
```

## Saving Module Configurations

After configuring the module and port settings, issue the SAVE MODULE\_PORT command from the management module to save the new configuration settings.

```
ONline> save module_port [ENTER]
```

## Reverting Module Configurations

Issue the REVERT command as shown to return a module to the configuration settings that were in effect as of the last save.

```
ONline> revert module_port [ENTER]
```

---

## Showing Module Configurations

You can display status information about the Security Module using the following management commands:

- ❑ SHOW MODULE
- ❑ SHOW MODULE VERBOSE
- ❑ SHOW PORT
- ❑ SHOW PORT VERBOSE

The following command displays detailed information about the Security Module in slot 3:

```
ONline> show module 3 verbose [ENTER]

Slot  Module          Version  Network      General Information
3      5112M-TPLS        001      ETHERNET_1

5112M-TPLS: ONline 10BASE-T Security Module

Network Dip Setting:          ETHERNET_1
Auto-partition Threshold:    63 COLLISIONS
```

The following command displays detailed information for port 1 on a Security Module in slot 12.

```
ONline> show port 12.1 verbose [ENTER]

Port Display for Module 5112M-TPLS :

Port  Mode          Status          Network      General Information
12.01 DISABLED    LINK FAILURE    ETHERNET_1
Port Alert:          ENABLED
Port Connector:      TELCO
Mode Dip Setting:    ENABLED
Security Dip Setting  DISABLED
Link Integrity Dip Setting:  ENABLED
```

The following output is an example of the SHOW PORT ALL VERBOSE command issued for the ports of a Security Module installed in slot 12 (only the output for ports 1, 2, and 3 are shown):

```
ONline> show port 12.all verbose [ENTER]

Port  Mode      Status              Network      General Information
-----
12.01  DISABLED LINK FAILURE  ISOLATED

Port Alert Filter:      DISABLED
Port Connector:         TELCO
Link Integrity:         ENABLED

12.02  DISABLED LINK FAILURE  ISOLATED

Port Alert Filter:      DISABLED
Port Connector:         TELCO
Link Integrity:         ENABLED

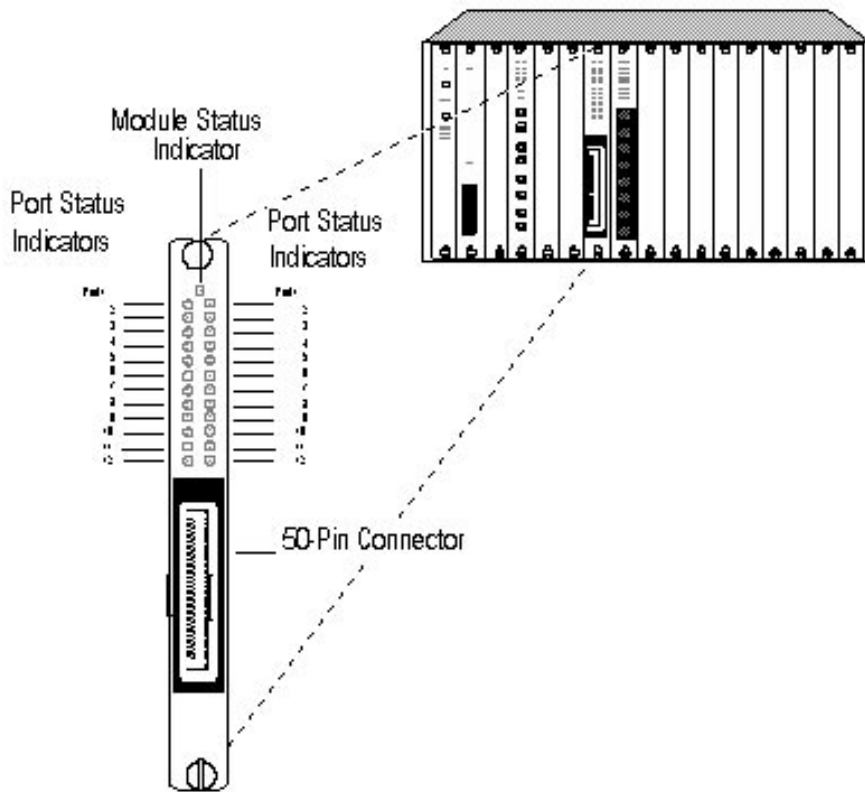
12.03  DISABLED LINK FAILURE  ISOLATED

Port Alert Filter:      DISABLED
Port Connector:         TELCO
Link Integrity:         ENABLED
```

---

# Monitoring the Front Panel

The Security Module has 12 Activity and 12 Status LEDs on the front panel that indicate the state of the ports. The LEDs allow you to monitor the status of each port. The front panel also contains a Module Status indicator that indicates the state of the module. Figure 3-5 shows the location the LEDs. Each LED indicates the state of its port as described in Table 3-4.



*Figure 3-6. Security Module Faceplate*

**Table 3-4. Interpretation of the Security Module LEDs**

LED Name	Color	State	Indicates
Activity (Ports 1-12)	yellow	Off	No packets are received on the segment.
		On	Constant activity on the segment.
		Blinking	Normal activity on the segment.
Status (Ports 1-12)	green	Off	Port disabled.
		On	Port enabled and link OK or Link Integrity disabled.
		1 blink	Link failure.
		2 blinks	Port partitioned.



---

## LED and Network Verification

Once the module is installed, verify its operation through the front panel of the ONline Controller Module. The Controller Module is equipped with an LED test button on the front panel. Use the LED test button to verify LED operation and verify network assignment.

When you press this button, the Controller Module initiates a test to all modules in the concentrator. All LEDs should respond by lighting continuously for approximately five seconds. Any LED that does not light is defective.

After the five seconds elapse, the diagnostic continues with a network check of all modules. Each Status LED should respond by blinking the number of times to correspond with the network to which the module is assigned. The network check sequence repeats five times. If a module is in isolated mode, the Status LEDs on the module remain off. The Activity LED remains on during the network check sequence. This test does not disrupt network operation. Table 3-5 explains the network check codes

***Table 3-5. Network Check Codes***

LED State	Network Configuration
1 Blink	Module is configured for network 1
2 Blinks	Module is configured for network 2
3 Blinks	Module is configured for network 3
Off	Isolated (module operates independent of any network)



# 4 *Configuring Security Features*

---

This chapter describes the security features of the ONline 10BASE-T Security Module and includes the management commands necessary to configure and monitor security functionality.

A master EMM at Version 4.0 is required to manage the features of the Security Module, including Autolearning. A master TRMM at Version 3.0 is required to manage the features of the Security Module *with the exception of the Autolearning Feature*. You must manually add MAC addresses to a port MAC address table in order for a TRMM to manage the security features of the Security Module. Refer to the section, Defining a MAC Address Manually, for a description of the command to add MAC addresses to a port MAC address table.

The remainder of this chapter describes:

- ❑ Configuring Security Features
- ❑ Showing Security Configurations
- ❑ Clearing Security Configurations
- ❑ Using the 3Com MIB Security Variables

---

## Quick Reference for Configuring Security

Table 4-1 outlines the steps necessary to configure the security features of your module. These procedures and command examples are explained further throughout this chapter. If you are familiar with these instructions, you may want to use this table as a checklist.

***Table 4-1. Quick Reference for Configuring the Security Module***

Procedure	Command
1. Disable Autolearning Mask to allow the EMM to Autolearn MAC addresses for ports. (Enabling Autolearning Mask prevents the EMM from learning a port's associated MAC addresses.)	SET SECURITY AUTOLEARN MASK
2. Disable Security Mode to allow the EMM to Autolearn MAC addresses for ports.	SET SECURITY PORT MODE
3. Enable the ports to allow traffic to pass through the network so the EMM can learn which MAC addresses are associated with which ports. (You must enable ports in order for Autolearning to run.)	SET PORT MODE

**Table 4-1. Quick Reference for Configuring the Security Module (Continued)**

Procedure	Command
4. Initiate Autolearning to enable the EMM to automatically learn the valid MAC addresses associated with a ports.	SET SECURITY AUTOLEARN CAPTURE
5. Download the learned MAC addresses from the Autolearning database to the port MAC address table.	SET SECURITY AUTOLEARN DOWNLOAD
<b>TRMM Note:</b> The TRMM does not support Autolearning. Therefore, you if you are using a TRMM to manage the Security Module, you must manually add MAC addresses to a port MAC address table.	SET SECURITY PORT MAC_ADDRESS
6. Define the Security type: Eavesdropping_only, Intrusion_only, or Full. <b>Note:</b> Security Mode is automatically enabled when you issue the SET SECURITY PORT SECURITY_TYPE command.	SET SECURITY PORT SECURITY_TYPE
7. Define the corrective action the EMM is to take upon a Security Intrusion attempt.	SET SECURITY PORT ACTION_ON_INTRUSION (only necessary if Security Type is set to Intrusion_Only or Full)
8. Save Security configuration values.	SAVE SECURITY

---

## Configuring Security Features

This section describes the security features of the Security Module, including Eavesdropping Security and Intrusion Detection. Included in this section are the features you must configure to enable security on the module:

- ☐ Define port security type
- ☐ Define port action on intrusion
- ☐ Configure Autolearning Mask
- ☐ Enable ports
- ☐ Configure autolearning
- ☐ Download the Autolearning database

Security configurations from the Security Module are automatically uploaded to a newly elected master management module or installation of a new master management module. This automatic uploading feature ensures that the Security Module configurations are always retained and eliminates the need for you to reconfigure the new master.

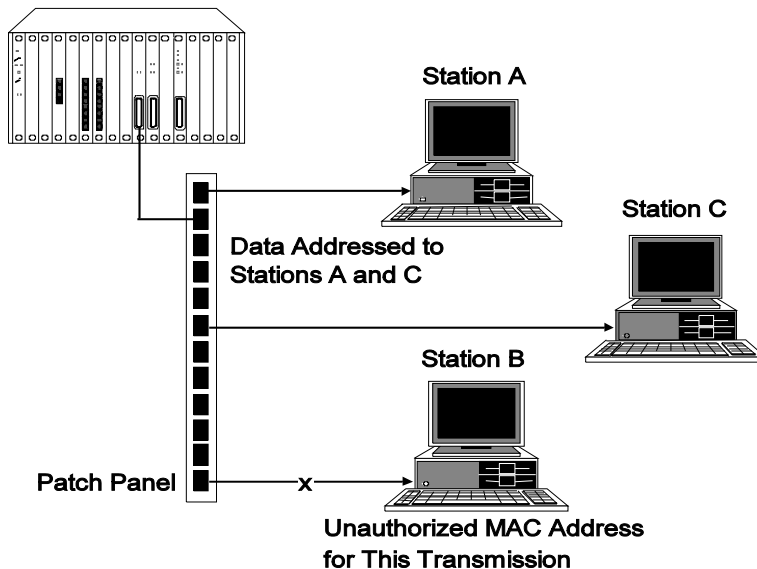
**Note:** If you issue security commands (with the exception of MAC address settings) specifying the 'all' option, all Security Module ports in the concentrator are affected by the command. If you are running an Advanced EMM, all other Ethernet modules in the concentrator that support security are also affected.

## Eavesdropping Security

Eavesdropping security is a port jamming feature that prevents users from accessing data transmitted to other users on the network. This type of security:

- ❑ Allows the Security Module to deliver packets only to the end station to which a packet is addressed.
- ❑ Prohibits unauthorized end stations from listening (eavesdropping) on packets that are not specifically addressed to them.

If a port receives a packet (from the ONLINE backplane) that is not targeted to any of the valid addresses associated with that port, the Security Module does not allow that packet to be delivered intact to the end station. Instead of delivering valid data to an unauthorized port, the module 'jams' the data by transmitting to the unauthorized port a data pattern of alternating zeros and ones.



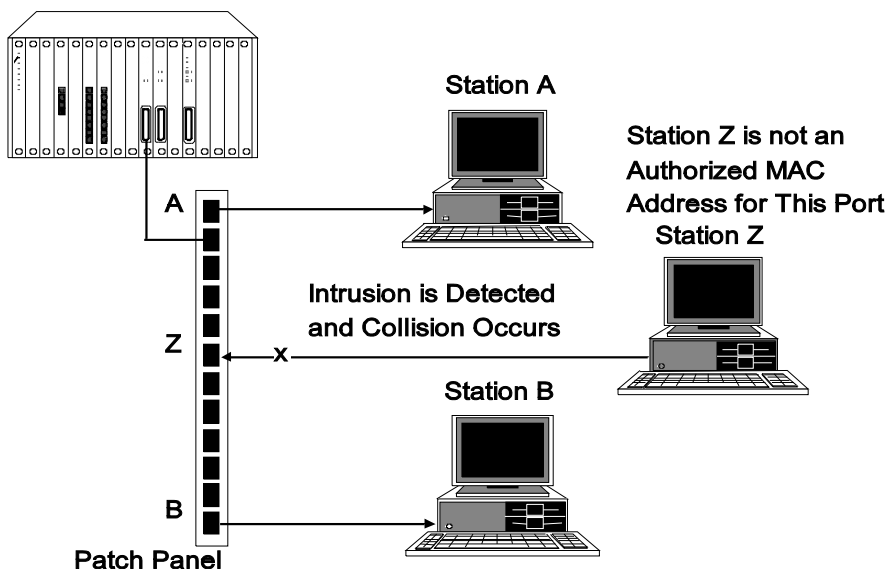
*Figure 4-1. Example of Eavesdropping Security*

## Intrusion Detection

Intrusion Detection allows the Security Module to prevent delivery of packets transmitted from unauthorized stations on the network. If a port receives a packet from its end station which contains an invalid source

address, the module forces a collision. The collision prevents intruding end stations from gaining access to a port and transmitting unauthorized data over the network.

Figure 4-2 illustrates an example of an Intrusion Detection configuration.



*Figure 4-2. Example of Intrusion Detection*

## Defining Port Security Type

You must define a security type for each port on the Security Module.

Issue the following command to configure the security type 'full' for all ports on the Security Module in slot 3.

```
Online> set security port 3.all security_type full [ENTER]
```

You may elect to configure ports for Eavesdropping Security only, Intrusion only, or Full (which includes both Eavesdropping and Intrusion). The default setting for Security Type is Full.



Security Mode is automatically enabled when you issue the SET SECURITY PORT SECURITY\_TYPE command.

Security Type is automatically configured to *Full* (which includes both Eavesdropping and Intrusion security) when you issue the SET SECURITY PORT MODE ENABLE command.

**Note:** Security mode must be *disabled* in order for the EMM to Autolearn MAC addresses for ports that have Security Type configured for Intrusion\_only or Full. If Security Mode is not disabled for each port that is configured for Intrusion Security:

- MAC addresses are not Autolearned
- The ports report an intrusion

## Defining Port Action on Intrusion

An additional feature of Intrusion Detection provides you with the ability to define on a per-port basis the corrective action a management module is to take when a Security Module port experiences a security intrusion attempt. Each option provides Intrusion Detection and data collision on the intruding packet. You may elect to have the management module perform one of the following actions:

- ☐ Disable the port and send a trap (disable\_and\_trap)
- ☐ Only disable the port (disable\_only)
- ☐ No management action (no\_action)
- ☐ Only send a trap to stations defined in the management module's community table (trap\_only)

Issue the following command to define disable\_and\_trap as the corrective action a management module will take upon a security Intrusion attempt for all ports on the module in slot 3.

```
ONline> set security port 3.all action_on_intrusion disable_and_trap [ENTER]
```

The default setting for action\_on\_intrusion is disable\_and\_trap.

**Note:** For a security intrusion attempt to be logged into the Intruder list, you must configure the action\_on\_intrusion setting for either disable\_and\_trap or trap\_only. Both settings allow a trap to be sent upon an intrusion, which also logs an entry into the Intruder list.

## Configuring Autolearning Mask

Autolearning Mask:

- ☐ Allows or prevents a port's MAC addresses from being learned by the EMM during Autolearning.
- ☐ Determines if the EMM is allowed or prevented from downloading learned MAC addresses to the ports.

The Autolearn Mask command either allows (disable the mask) or prevents (enable the mask) the EMM from learning or downloading MAC addresses for ports.

Issue the following command to allow the EMM to learn MAC addresses during Autolearning for all ports on the Security Module in slot 3.

```
ONline> set security autolearn 3.all mask disable [ENTER]
```

## Enabling Ports

For an EMM to learn MAC addresses for ports through Autolearning, the ports must be enabled (at some point) to allow network traffic to pass through. Therefore, ensure that ports are enabled prior to initiating Autolearning. Note that Autolearning will run on a disabled port, however, no MAC addresses will be learned.

Issue the following command to enable all the ports on the Security Module in slot 3.

```
ONline> set port 3.all mode enable [ENTER]
```

## Configuring Autolearning

Autolearning uses the network monitoring features of the EMM to provide a mechanism which:

- ☐ Learns the MAC addresses of the stations that have been sending packets to the EMM network
- ☐ Continuously monitors network activity

An EMM at Version 4.0 is required to configure Autolearning.

Once the Autolearning capture process begins, the EMM takes an instantaneous 'snapshot' of the MAC addresses that have passed through the specified ports. These addresses are stored in the Autolearning database.

Issue the following command to initiate Autolearning capture for all ports on the Security Module in slot 3.

```
ONline> set security autolearn 3.all capture [ENTER]
```

The following steps are initiated once the Autolearn Capture command is issued:

1. The Autolearning database (the storage area for learned MAC addresses) is cleared.
2. All of the MAC addresses observed on the specified ports are entered into the Autolearning database.
3. The entries from the specified ports' MAC address table are copied into the Autolearning database.

4. The result of this copy is a combination of the existing MAC addresses associated with a port, and the MAC addresses recently learned. (Remember that a port must have its Autolearning Mask disabled in order for MAC addresses to be learned.)
5. If MAC addresses for the specified ports currently exist in the Autolearning database, the following message is displayed when the Autolearn Capture command is issued:

`Note: overwriting previously autolearned addresses.`

If no MAC addresses were learned for the specified ports, then the following message is displayed:

`Autolearn capture done; learned 0 addresses total.`

6. Upon completion of Autolearning, the following message is displayed:

`Autolearn capture done; learned x addresses total.`

(where x indicates the total number of addresses now stored in the Autolearning Database)

The stored MAC addresses are now ready to be downloaded to the Security Module ports. Refer to the section, *Downloading the Autolearning Database*, further in this chapter.

**Note:** Security Mode must be *disabled* in order for the EMM to Autolearn MAC addresses for ports that are configured for Security Types *Intrusion\_only* or *Full*. If Security mode is not disabled for each port that is configured for Intrusion Security:

- MAC addresses will not be Autolearned
- The ports will report an intrusion

## Defining a MAC Address Manually

The Security Module provides you with the flexibility of manually adding MAC addresses into a port's MAC address table, and into the Autolearning Database. You may use this feature to add one or more MAC addresses to a port MAC address table instead of Autolearning a port's associated MAC addresses.

**Note:** If you are using a TRMM to manage the Security Module, you must use this command in order to add MAC addresses to a port MAC address table. (The TRMM does not support Autolearning.)

For example, once Autolearning Capture has completed and the MAC addresses are downloaded, a new station may be added to the network. You can add the new station's MAC address to a port's MAC address table using the SET SECURITY PORT MAC\_ADDRESS command.

Issue the following command to add the MAC address 08-54-6f-01-32-08 to the MAC address table for port 1 on the module in slot 3.

```
ONline> set security port 3.1 mac_address 08-54-6f-01-32-08 [ENTER]
```

**Note:** MAC addresses 00-00-00-00-00-00 and FF-FF-FF-FF-FF-FF are invalid.

Use the following command to add the MAC address 08-54-6f-01-32-08 into the Autolearning database. This command specifies that port 1 on the Security Module in slot 3 is associated with the MAC address 08-54-6f-01-32-08.

```
ONline> set security autolearn 3.1 mac_address 08-54-6f-01-32-08 [ENTER]
```

## Downloading the Autolearning Database

You must download the contents of the Autolearning database to the Security Module ports in order for the MAC Addresses to be associated with the ports. When Autolearning Capture is complete, download the Autolearning database to initiate port security. Depending on the amount of network traffic transmitted to the Security Module ports, you may elect to defer the Autolearn download for a day, several days, or a week. Waiting to download the captured MAC addresses allows all of a port's associated MAC addresses to be entered into the Autolearning database.

The Autolearning database for an EMM can contain a maximum of 360 MAC addresses. The Autolearning database for a TRMM can contain a maximum of 400 MAC addresses.

Since a maximum of four MAC addresses can be associated with one port, only four MAC addresses are downloaded. The four MAC addresses with the lowest alpha-numerical values are downloaded from the Autolearning database to a Security Module ports.

Issue the following command to download the Autolearning database to port 1 on the Security Module in slot 3.

```
ONline> set security autolearn 3.1 download [ENTER]
```

If MAC addresses for the specified port currently exists in the port MAC address table, the following message is displayed when the Autolearn Download command is issued:

```
Note: overwriting existing addresses in the Security database.
```

The following message is displayed upon completion of the Autolearn Download command (where y indicates the total number of addresses copied to the port's MAC address table):

```
Autolearn download done; downloaded y addresses total.
```

If a port has more than four MAC addresses in the Autolearning database at the time of the download, the following message displays upon completion of the Autolearn Download command:

Note: at least one autolearned address was skipped because the port with which it is associated has more than 4 autolearned addresses.

If any MAC address was skipped because the concentrator limit was reached, the following message displays upon completion of the Autolearn Download command:

Note: the number of autolearned addresses exceeds the concentrator limit. Only the first X addresses (as ordered by slot, port, and addr) were downloaded.

Where x indicates 360 MAC addresses for an EMM or 400 MAC addresses for TRMM.

## Configuring Security Mode

The Security Module provides you with the flexibility of manually enabling or disabling Security Mode for ports. Security Mode is enabled *automatically* for the ports specified in the SET SECURITY PORT SECURITY\_TYPE command.

Issue the following command to enable security for all ports on the Security Module in slot 3.

```
ONline> set security port 3.all mode enable [ENTER]
```

Security Type is automatically configured to *Full* (which includes both Eavesdropping and Intrusion security) when you issue the SET SECURITY PORT MODE ENABLE command.

You may enable Security mode for a port that does not have secure MAC addresses associated with it. However, each packet received by a port will have an invalid MAC address assigned and will therefore be treated as an intrusion.

Note that Security Mode must be *disabled* in order for the EMM to Autolearn MAC addresses for ports that are configured for Security Types Intrusion or Full. If Security mode is not disabled for each port that is configured for Intrusion Security:

- ❑ MAC addresses will not be Autolearned
- ❑ The port(s) will report an intrusion. (An intrusion is only reported if a port Action\_on\_intrusion setting is configured to either Disable\_and\_trap or Trap\_only.)

## Saving Security Configurations

The SAVE SECURITY command saves all security information for each port on every Security Module, and on every Ethernet module in the concentrator. Issue the following command to save security configurations and make the information permanent.

```
Online> save security [ENTER]
```

## Reverting Security Configurations

The REVERT SECURITY command reverts all security information for all ports on all Security Modules, and on all Ethernet modules in the concentrator to their previously saved settings. Issue the following command to revert security configurations.

```
Online> revert security [ENTER]
```

---

## Showing Security Configurations

The Security Module provides several SHOW commands that display:

- ❑ Port security configurations for a single port, all ports on a Security Module, or all ports on all Security Modules in a concentrator
- ❑ Entries in the Autolearning database
- ❑ All entries in the Security Intruder list

The SHOW commands to display this information are described in the following sections.



## Showing Port Configurations

You can display information about the Security Module ports using the SHOW PORT SECURITY command. The following command displays:

- All of the addresses (up to four per-port) for a single port or
- All 12 ports on a Security Module or
- All ports on all Security Modules in a concentrator

The command example shown displays security information for all ports on the Security Module in slot 17.

```
ONline> show security port 17.all [ENTER]
```

Security Display for Module 5112M-TPLS in Slot 17:

<u>Port</u>	<u>Mode</u>	<u>MAC Addresses</u>	<u>General Information</u>
17.01	DISABLED	17-01-01-01-01-01	ETHERNET_1
17.02	EAVESDROP	NONE	ETHERNET_1
17.03	INTRUSION	01-02-03-04-05-06 01-02-03-04-05-07	ETHERNET_1
17.04	FULL	NONE	ETHERNET_1
17.05	FULL	NONE	ETHERNET_1
17.06	FULL	NONE	ETHERNET_1
17.07	FULL	NONE	ETHERNET_1
17.08	FULL	03-02-01-00-09-08 03-02-01-00-09-09 03-02-01-00-09-0a	ETHERNET_1
17.09	FULL	NONE	ETHERNET_1
17.10	FULL	NONE	ETHERNET_1
17.11	FULL	NONE	ETHERNET_1
17.12	DISABLED	NONE	ETHERNET_1

The command example shown displays all security information, including configuration settings, for all ports on the Security Module in slot 17 (only 6 of the 12 ports are shown).

Online> show security port 17.all verbose [ENTER]

Security Display for Module 5112M-TPLS in Slot 17 :

Port	Mode	MAC Addresses	General Information
17.01	DISABLED	17-01-01-01-01-01	ETHERNET_1
Port Action On Intrusion:			DISABLE_AND_TRAP
Autolearn Mask:			ENABLED
17.02	EAVESDROP	NONE	ETHERNET_1
Port Action On Intrusion:			DISABLE_ONLY
Autolearn Mask:			DISABLED
17.03	INTRUSION	01-02-03-04-05-06 01-02-03-04-05-07	ETHERNET_1
Port Action On Intrusion:			TRAP_ONLY
Autolearn Mask:			DISABLED
17.04	FULL	NONE	ETHERNET_1
Port Action On Intrusion:			NO_ACTION
Autolearn Mask:			DISABLED
17.05	FULL	NONE	ETHERNET_1
Port Action On Intrusion:			DISABLE_AND_TRAP
Autolearn Mask:			DISABLED
17.06	FULL	03-02-01-00-09-08 03-02-01-00-09-09 03-02-01-00-09-0a	ETHERNET_1
Port Action On Intrusion:			DISABLE_AND_TRAP
Autolearn Mask:			DISABLED

## Showing Security Autolearn

The SHOW SECURITY AUTOLEARN command displays all of the MAC addresses that have been learned and stored in the Autolearning database. Only entries for ports specified in the command are displayed. An additional message is provided if any port has more than four entries, or if the concentrator limit has been exceeded.

To display all associated MAC addresses for the ports on the Security Module in slot 17, issue the following command.

```
ONline> show security autolearn 17.all [ENTER]
```

```
Autolearned Addresses for Module 5112M-TPLS in Slot 17 :
```

<u>Port</u>	<u>MAC Address(s)</u>
17.01	01-01-01-01-01-01
17.06	08-00-8f-01-02-03
	08-00-8f-02-03-04
	08-00-8f-04-05-06
	08-00-8f-05-06-07
	08-00-8f-06-07-08 *
	08-01-01-01-01-01 *
17.09	09-00-8c-09-09-09
	09-00-8c-09-09-0a
17.12	12-00-01-12-12-12

Note: at least one port on this module has more than 4 security addresses autolearned for it. Only the first 4 addresses per port (as ordered by MAC address) will be downloaded; extraneous address are marked in the display above with an asterisk.

A single asterisk (\*) marks entries for a port that exceeds the maximum of four MAC addresses per port.

If the number of MAC addresses learned exceeds the concentrator limit, the following message is displayed:

Note: The number of autolearned addresses exceeds the concentrator limit. Only the first x addresses (as ordered by slot, port, and addr) will be downloaded. Extraneous addresses are marked with a double asterisk.

A double asterisk (\*\*) marks entries that have exceeded the EMM capacity of 360 MAC addresses, or the TRMM capacity of 400 MAC addresses. Entries that exceed the 360 or 400 MAC address maximum (that is, entry 361 and greater or entry 401 or greater) are not downloaded.

If your concentrator is near full capacity, or if you have ports connected to bridges, you may wish to perform two or more Autolearn Captures, which may prevent these ports from exceeding the 360 MAC address limit.

For example, to perform two Autolearn Captures:

1. Initiate an Autolearn Capture specifying only some of the modules and ports.
2. Download this information to the Security Module.
3. Initiate the second Autolearn Capture specifying the remaining modules and ports.
4. Download this information to the Security Module.

## Showing Security Intruder List

The SHOW SECURITY INTRUDER\_LIST command is only available with Advanced EMM Version 4.0. The Security Intruder list contains information regarding the 10 most recent intrusion attempts for a network. This information includes:

- ☐ The MAC address of the intruding station (MAC addresses are available for all Ethernet modules with the exception of the Security Module)
- ☐ The time that has elapsed since the intrusion attempt occurred (in days, hours, minutes, and seconds)
- ☐ A notification if the port was automatically disabled

The oldest entry in the Intruder list is removed when the list is full (10 entries) and a new intrusion attempt occurs.

The following command example displays a Security Intrusion list for a two-port 10BASE-FB Module.

```
ONline> show security intruder_list [ENTER]
```

Port	MAC Address	Time Since Intrusion				Auto-Disable?
03.01	08-00-8f-02-c6-be	0d	0h	15m	27s	YES
03.02	09-d3-74-00-2e-01	1d	5h	32m	53s	YES

MAC addresses for unauthorized stations that attempt to transmit data to Security Module ports are not displayed. The MAC addresses are not displayed because the MAC address is intercepted by Intrusion Detection, and cannot reach the network where the EMM can detect the MAC address.

---

# Clearing Security Configurations

The Security Module provides commands to clear a MAC address from a port's MAC address table, and from the Autolearning Database. A cleared MAC address is no longer considered to be a valid address. A command is also available to clear the Security Intruder list.

## Clearing the MAC Address Table

You may want to manually clear a MAC address from a port instead of initiating Autolearning to recapture a port's associated MAC addresses. For example, once Autolearning Capture has completed and the information downloaded, a station may be removed from the network.

Issue the following command to clear the MAC address 08-54-6f-01-32-08 from the MAC address table for port 1 on the Security Module in slot 3.

```
ONline> clear security port 3.1 mac_address 08-54-6f-01-32-08 [ENTER]
```

Use the All option to remove all associated MAC addresses from a specific port, all ports on a Security Module, or all ports on all Security Modules in a concentrator. If you do not enter a MAC address, the command defaults to All, which clears all MAC addresses from the specified ports.

**Note:** Security Mode is not disabled automatically when you delete a port's MAC address. Thus, a port may not have a MAC address associated with it *yet still have security enabled*. In this case, any end station attached to that port is deemed "unauthorized." Always disable Security Mode on a port that does not have an assigned MAC address.

## Clearing the Autolearning Database

Issue the following command to clear from the Autolearning database all MAC addresses associated with port 1 on the Security Module in slot 3.

```
ONline> clear security autolearn 3.1 mac_address all [ENTER]
```

If you do not enter a MAC address, the command defaults to All, which clears all MAC addresses from the Autolearning database for the specified ports.

## Clearing the Security Intruder List

The Security Intruder list contains information regarding the 10 most recent intrusion attempts. Use the following command to completely clear the Intruder list.

```
ONline> clear security intruder_list [ENTER]
```

```
Intruder List cleared.
```

---

## Using 3Com MIB Security Variables

This section lists the network management Security MIB (Management Information Base) variables and the ONline 10BASE-T Security Module MIB variables.

### EMM Security SNMP Variables

The MIB variables for the EMM Security settings include:

- ❑ **olNetSecurityMACTable** - Table of security information for the entire concentrator.
- ❑ **olNetSecurityMACEntry** - The element type for entries in the olNetSecurityMACTable. An entry consists of a:
  - slot number
  - port number
  - single MAC address
  - mode value
  - status value
- ❑ **olNetSecurityMACSlotIndex** - The slot number, defined to be an integer.
- ❑ **olNetSecurityMACPortIndex** - The port number, defined to be an integer.
- ❑ **olNetSecurityMACAddress** - Defines the MAC address to be a 6-byte field.
- ❑ **olNetSecurityMACMode** - Defines the possible mode values that may be associated with a port. Currently, only Enable and Disable are defined as legitimate values. These values indicate if security is enabled for a port.

- ❑ **olNetSecurityMACStatus** - Status associated with each port, which indicates if a valid (non-zero) MAC address is assigned to it. The possible values for this field are Valid and Invalid.

## Using the Security Module SNMP Variables

Listed below are the MIB (Management Information Base) variables for the ONline 10BASE-T Security Module.

- ❑ **ol51nnMTPLSModTable** - List of module-specific information about a specific 51nnM-TPLS module in the concentrator.
- ❑ **ol51nnMTPLSModEntry** - List of module-specific information about a specific 51nnM-TPLS module in the concentrator.
- ❑ **ol51nnMTPLSModSlotIndex** - Slot number of this module.
- ❑ **ol51nnMTPLSModDipNetwork** - Network indicated by the module's dip switches.
- ❑ **ol51nnMTPLSModDipSecurity** - Module security configuration as indicated by this module's DIP switches.
- ❑ **ol51nnMTPLSModAutoPartition** - Holds the consecutive collision count limit value.
- ❑ **ol51nnMTPLSPortTable** - Table of port-specific information for each port of this module type.
- ❑ **ol51nnMTPLSPortEntry** - List of module-specific information about a specific 51nnM-TPLS port in the concentrator.
- ❑ **ol51nnMTPLSPortSlotIndex** - Slot number of this port's module.
- ❑ **ol51nnMTPLSPortAdminState** - The desired state of this port.
- ❑ **ol51nnMTPLSPortBuddySlot** - The slot index of the redundant port's buddy.



- ❑ **ol51nnMTPLSPortBuddyPort** - The port index of the redundant port's buddy.
- ❑ **ol51nnMTPLSPortLinkInteg** - The link integrity configuration for this port.
- ❑ **ol51nnMTPLSPortDipLinkInteg** - The link integrity configuration for this port as indicated by the module DIP switch setting.



# 5 *Troubleshooting*

---

This chapter describes troubleshooting procedures for the ONline Security Module. Information on troubleshooting will assist you in verifying operation. Typical fault conditions are addressed in this chapter.

---

## Troubleshooting

Diagnostic features have been covered to a large extent in Tables 3-4 and 3-5. Table 5-1 and Table 5-2 in this chapter cover fault conditions and troubleshooting suggestions for the ONline 10BASE-T Security Module. This chapter is divided into the following sections:

- ❑ Troubleshooting Using the Port Status LEDs
- ❑ Troubleshooting Using the Activity LEDs
- ❑ Technical Assistance

## Troubleshooting Using the Status LEDs

A blinking Port Status indicator (LED) signals a problem with a port or a link connected to a port. Once a port detects a problem, you can further analyze the problem by counting the number of blinks. Table 5-1 provides troubleshooting suggestions for each of the blinking sequences.

**Note:** The LEDs provide accurate information only when unused ports are disabled.

**Table 5-1. Troubleshooting Using the Port Status LEDs**

LED State	Indication	Possible Problem	Troubleshooting Suggestions
1 Blink	Link Failure	Cables not connected.	Connect cables.
		Cables broken.	Check cables with cable tester. Repair or replace cables.
		Link Integrity mismatch.	Make sure that both ends of the connection have the same Link Integrity setting.
2 Blinks	Port Partitioned	Faulty cable.	Check cable with cable tester. Repair or replace cable.
		Network overloaded.	Reassign users to another network to balance the load.
Off	Ports Disabled	Ports disabled.	Enable ports.
		Security Module not powered.	Check the Controller Module Power LEDs.

***Table 5-1. Troubleshooting Using the Port Status LEDs (Continued)***

<b>LED State</b>	<b>Indication</b>	<b>Possible Problem</b>	<b>Troubleshooting Suggestions</b>
Off (continued)	Ports Disabled (continued)	Broken LED.	Press the LED test on the Controller Module.
		Faulty Security Module.	Replace module.
		Attempted breach of security intrusion.	Display the Intruder list for intruder information. Then re-enable the port.

The Security Module also provides a Module Status LED. This LED indicates the operational status of the module. The Module Status LED is On to indicate the module is operational. The LED is Off to indicate the module is non operational. If this LED is off, refer to the troubleshooting suggestions in Table 5-1.

This LED is helpful if the Security Module is first installed, but the Autolearning database has not been downloaded to the module. The Module Status LED will be On and the 12 Port Status LEDs will be Off, indicating that the Security Module is operational, but all 12 ports are disabled. Thus, the Module Status LED enables you to discern that the lack of bus traffic is due to the ports being disabled rather than due to a fault with the Security Module.

## Troubleshooting Using the Activity LEDs

Under some conditions a port Activity LED may not light. Use the troubleshooting suggestions in Table 5-2 to help determine why the light is off, and to isolate the source of the problem.

***Table 5-2. Troubleshooting Using the Activity LEDs***

LED State	Possible Problem	Troubleshooting Solutions
Off	There is no traffic received from the segments (normal).	None.
	Concentrator power is Off.	Check the Controller Module Power LEDs.
	The Activity LED has burned out.	Press the LED test button on the Controller Module.
	A Security Module port is faulty.	Connect the cable to a different port.
	The module connection to the backplane is bad.	Reinsert the Security Module. If this fails to correct the problem, try another concentrator slot.
	The Security Module is faulty.	Try a different Security Module.

---

## Technical Assistance

You can receive assistance for installing and troubleshooting the Security Module by calling either your 3Com reseller or 3Com Technical Support. Be prepared to supply a representative with the following information:

- ☐ Description of the problem
- ☐ Steps you have taken to try and correct the problem
- ☐ Type and software version of the ONline network management module being used
- ☐ Version of software installed on your Security Module
- ☐ Status of the front panel LEDs
- ☐ Configuration of your network
- ☐ Configuration of your concentrator  
(you may find it helpful to refer to the Slot Usage Chart in Appendix B of the *ONline System Concentrator Installation and Operation Guide* for a record of this information)

Refer to Appendix B for instructions on contacting Technical Support for your product.





# A *Specifications*

---

This appendix lists:

- ☐ Electrical Specifications
- ☐ Environmental Specifications
- ☐ Mechanical Specifications
- ☐ General Specifications
- ☐ 50-Pin Connector and Cable
- ☐ Twisted Pair Connectors and Cables

---

## **Electrical Specifications**

Backplane Interface: 96-pin edge connector, compatible with the 3Com ONline System Concentrators.

Power Requirements: 2.0 A for 5V

Fuse: 4.0 Amps Fast blow

Watts: 10

---

## Environmental Specifications

Operating Temperature: 0° to 50° C (32° to 122° F)

Storage Temperature: -30° to 65° C (-22° to 149° F)

Humidity: less than 95%, non-condensing

BTU/hr: 34

---

## Mechanical Specifications

Dimensions: 1.0" W x 10.25" L x 8.5" H

(2.54 cm x 26.04 cm x 21.6 cm)

Weight: 1.25 lb. (0.57 kg.)

---

## General Specifications

Data rate: 10 Mbps (million bits per second)

Data modulation: Manchester

Diagnostic modulation: Link Integrity pulse

Collision detection: 100% deterministic

Port partitioning: user-settable

Maximum number of nodes: 1024

Configuration rules: supports IEEE 802.3 controllers and IEEE 802.3 repeaters

Jabber protection: 6.5 milliseconds

Ethernet interface: 50-pin TELCO connector; supports 12 connections

Number of ports: 12

Cabling: conforms to the 10BASE-T standard

Cable differential impedance: 85 ohms to 115 ohms over 1 to 16 MHz band

Cable propagation velocity:  $>.585c$

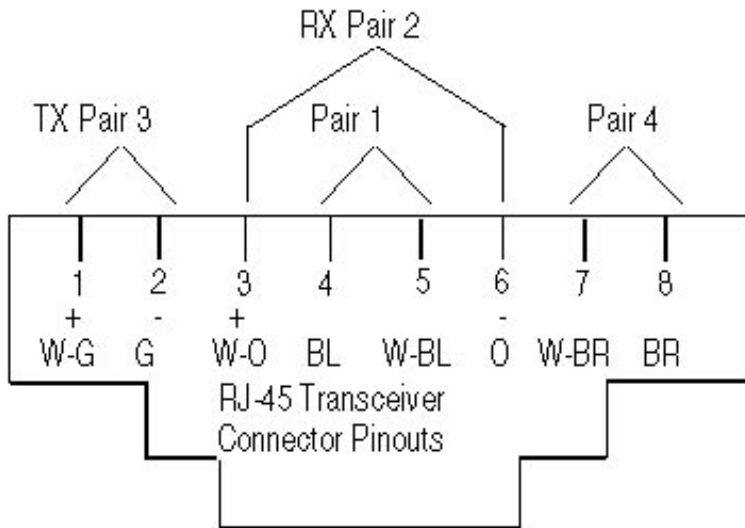
Host interface: 3Com ONline System Concentrator bus interface standard

Installation attachment: Two thumbscrews on the mounting bracket

---

## 50-Pin Connector and Cable

Figure A-1 illustrates the cable pinouts for the Security Module female connector and the 50-Pin cable male connector. This figure also shows how to connect Port 1 of the Security Module to a desktop transceiver using the TIA-568A wiring standard for an RJ-45 connection. Connections between the module and the desktop device can be made through a patch panel, Hydra cable, or punchdown block. It is critical that the data path be preserved along the route from the module's Telco connector to the remote end, especially when going through patch panels or punchdown blocks.



**Figure A-1. 50-Pin Cable Male and Female Connectors**

Table A-1 lists the pinouts, receive/transmit pairs and polarity, and port assignments for the 50-Pin Telco cable that connects to the Security Module.

**Table A-1. 50-Pin Cable Pinouts and Port Assignments**

<b>Hub Port #</b>	<b>Hub Pin #</b>	<b>Hub Function /Polarity</b>	<b>Trans-ceiver Function /Polarity</b>	<b>Hub Port #</b>	<b>Hub Pin#</b>	<b>Hub Function /Polarity</b>	<b>Trans-ceiver Function /Polarity</b>
Port 1	26	RX, +	TX, + (1)	Port 7	38	RX, +	TX, + (1)
Port 1	1	RX, -	TX, - (2)	Port 7	13	RX, -	TX, - (2)
Port 1	27	TX, +	RX, + (3)	Port 7	39	TX, +	RX, + (3)
Port 1	2	TX, -	RX, - (6)	Port 7	14	TX, -	RX, - (6)
Port 2	28	RX, +	TX, + (1)	Port 8	40	RX, +	TX, + (1)
Port 2	3	RX, -	TX, - (2)	Port 8	15	RX, -	TX, - (2)
Port 2	29	TX, +	RX, + (3)	Port 8	41	TX, +	RX, + (3)
Port 2	4	TX, -	RX, - (6)	Port 8	16	TX, -	RX, - (6)
Port 3	30	RX, +	TX, + (1)	Port 9	42	RX, +	TX, + (1)
Port 3	5	RX, -	TX, - (2)	Port 9	17	RX, -	TX, - (2)
Port 3	31	TX, +	RX, + (3)	Port 9	43	TX, +	RX, + (3)
Port 3	6	TX, -	RX, - (6)	Port 9	18	TX, -	RX, - (6)
Port 4	32	RX, +	TX, + (1)	Port 10	44	RX, +	TX, + (1)
Port 4	7	RX, -	TX, - (2)	Port 10	19	RX, -	TX, - (2)
Port 4	33	TX, +	RX, + (3)	Port 10	45	TX, +	RX, + (3)
Port 4	8	TX, -	RX, - (6)	Port 10	20	TX, -	RX, - (6)
Port 5	34	RX, +	TX, + (1)	Port 11	46	RX, +	TX, + (1)
Port 5	9	RX, -	TX, - (2)	Port 11	21	RX, -	TX, - (2)

**Table A-1. 50-Pin Cable Pinouts and Port Assignments (Continued)**

Hub Port #	Hub Pin #	Hub Function /Polarity	Trans-ceiver Function /Polarity	Hub Port #	Hub Pin#	Hub Function /Polarity	Trans-ceiver Function /Polarity
Port 5	35	TX, +	RX, + (3)	Port 11	47	TX, +	RX, + (3)
Port 5	10	TX, -	RX, - (6)	Port 11	22	TX, -	RX, - (6)
Port 6	36	RX, +	TX, + (1)	Port 12	48	RX, +	TX, + (1)
Port 6	11	RX, -	TX, - (2)	Port 12	23	RX, -	TX, - (2)
Port 6	37	TX, +	RX, + (3)	Port 12	49	TX, +	RX, + (3)
Port 6	12	TX, -	RX, - (6)	Port 12	24	TX, -	RX, - (6)
					50	Not Used	Not Used
					25	Not Used	Not Used

## Twisted Pair Connectors and Cables

You can use many types of cables and connectors to link your Security Module to your network. Use the information in this section to ensure that the cables and connecting hardware meet requirements.

**Note:** For proper operation, use only approved cables when you install all equipment.

3Com recommends that you connect cables first at the active concentrator location, and connect transceivers second. Refer to the *ONline System Concentrator Installation and Operation Guide* for more information about the ONline System Concentrator connections.

This section is divided into the following parts:

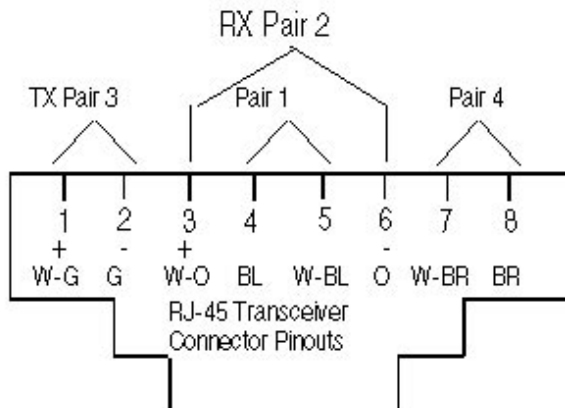
- ❑ Twisted Pair Connectors
- ❑ Twisted Pair Cables

## Twisted Pair Connectors

Use the IEEE 802.3 10BASE-T standard for RJ-45 pinouts as described below. 10BASE-T uses 2 of the 4 pairs of wire: pins 1 and 2 and pins 3 and 6. If the pairs are not configured this way, the connection will not work properly. Level 3 or higher cable should have the following pin pairings:

- ❑ pins 4 and 5 are pair 1
- ❑ pins 3 and 6 are pair 2
- ❑ pins 1 and 2 are pair 3
- ❑ pins 7 and 8 are pair 4

Refer to Figure A-1 for an example of the recommended TIA-568A wiring standard for an RJ-45 connector.



**Figure A-2. RJ-45 Connector Pinouts**

Some installations may have 50-pin Telco connectors at the wiring closet. We recommend using a patch panel that converts from 50-pin to RJ45-type connectors. This allows direct connection to the Security Module in your ONline System Concentrator.

## Twisted Pair Cables

The cables that are supported must meet the following qualifications:

- ☐ Level 3 or higher
- ☐ 22 or 24 gauge twisted pair cable
- ☐ 85 to 115 ohm impedance
- ☐ minimum of 2 pairs

A pair is usually a solid color wire twisted with a striped wire with the same color.



# B *Technical Support*

---

3Com provides easy access to technical support information through a variety of services. This appendix describes the following services:

- ☐ On-line Technical Support
- ☐ Support from Your Network Supplier
- ☐ Support from 3Com
- ☐ Returning Products for Repair
- ☐ Accessing the 3Com MIB
- ☐ 3Com Technical Publications

---

## **On-line Technical Support**

3Com offers worldwide product support through the following on-line systems:

- ☐ Email Technical Service
- ☐ World Wide Web Site

## Email Technical Support

You can contact the Integrated Systems Division (formerly Chipcom) on the Internet for technical support using the e-mail address [techsupp@chipcom.com](mailto:techsupp@chipcom.com).

## World Wide Web Site

You can access the latest networking information on the 3Com World Wide Web site by entering our URL into your Internet browser:

**<http://www.3Com.com/>**

This service features news and information about 3Com products, customer service and support, the 3Com latest news releases, selected articles from 3TECH™, the 3Com award-winning technical journal, and more.

You can contact the Integrated Systems Division on the World Wide Web by entering our URL into your Internet browser:

**<http://www.chipcom.com/>**

There are links between both WWW pages to view information from all 3Com divisions.

---

## Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- ☐ Diagnostic error messages
- ☐ A list of system hardware and software, including revision levels
- ☐ Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

---

# Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

For direct access to customer service for Integrated Systems Division products in:

- ☐ U.S.A. and Canada - call (800) 724-2447
- ☐ Asia Pacific - call (508) 787-5151
- ☐ Europe - refer to the table below. For European countries not listed, call 31 30 60 299 00

Country	Telephone Number
Belgium	0800 71429
Denmark	800 17309
Finland	0800 113153
France	05 917959
Germany	0130 821502
Ireland	1 800 553117
Italy	1678 79489

Country	Telephone Number
Netherlands	06 0227788
Norway	800 11376
Spain	900 983125
Sweden	020 795482
U.K.	0800 966197
U.S.	800 876-3266

For access to customer service for all 3Com products, call (800) 876-3266.

You can also contact the Integrated Systems Division (ISD) on the Internet by using the e-mail address [techsupp@chipcom.com](mailto:techsupp@chipcom.com).

---

## Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number for Integrated Systems Division products (formerly Chipcom), use the following numbers.

Country	Telephone Number	Fax Number
U.S. and Canada	(800) 724-2447	(508) 787-3400
Europe	(44) (1442) 275860	No Fax
Asia Pacific	(508) 787-5296	(508) 787-3400

---

## Accessing the 3Com MIB

The 3Com Management Information Base (MIB) for the Integrated Systems Division describes commands that enable you to manage 3Com SNMP-based products. The MIB is available over the Internet on an anonymous FTP server. Updates to these MIBs are released as new 3Com products are introduced.

To access Internet versions:

1. FTP to `ftp.chipcom.com` (151.104.9.65).
2. Enter the login name `anonymous`.

3. Enter your full Internet e-mail address as the password (for example, `jdoe@company.com`).
4. Change to the `mib` or `schema` directory using the `cd /pub/mibs` or `cd /pub/mibs/schemas` command.
5. To view the 3Com MIB, OID, or schema entries, enter the `dir` command.
  - ❑ To pause the display, press [CTRL-S].
  - ❑ To continue the display, press [CTRL-Q].
6. Copy the MIB, OID, or schema files to your current directory using the appropriate command (for example, `get chipcom.mib`).
7. To exit the FTP session, invoke the `quit` command.

---

## 3Com Technical Publications

If you have comments or questions on 3Com Integrated Systems Division Technical Publications documents, please contact the Technical Publications group by FAX (508) 229-1551.



# Index

## ***Numerics***

- 10BASE-T
  - Signalling Standard, 1-1
  - Transceivers, 2-8
- 3Com Bulletin Board Service (3ComBBS), B-3
- 50-Pin Cable
  - Pinouts and Port Assignments, A-5
- 50-Pin Connector, A-3

## ***A***

- Activity LEDs
  - Troubleshooting With, 5-4
- Audience of Manual, xiii
- Autolearning, 1-3, 4-8
  - Capture, 4-9
  - Configuring, 4-9
  - Database, 4-9
  - Ports, 4-8
  - Security Mode Setting, 4-10, 4-13
  - Using Security Mode, 4-7
- Autolearning Capture
  - Messages, 4-10
- Autolearning Database, 4-9, 4-19
  - Downloading, 4-12
  - Maximum Entries, 4-12
- Autolearning Mask
  - Configuring, 4-8
  - Considerations, 4-10
- Autopartition Threshold
  - Configuring, 3-16
  - Default, 3-16

## ***B***

- Backbone
  - Fiber Medium, 2-2
- Bridges, 2-8
- bulletin board service, B-3

## ***C***

- Cabling
  - Fiber Backbone, 2-7, 2-9
  - Pin Pairings, A-7
  - Twisted Pair Backbone, 2-10
  - Wire Types, A-8
- Clear Security Intruder List Command, 4-20
- Clear Security Port MAC Address Command, 4-19
- Clearing Security Configurations, 4-19
- Commands
  - Clear Security Intruder List, 4-20
  - Clear Security Port MAC Address, 4-19
  - Revert Security, 4-14
  - Save Security, 4-14
  - Set Module Autopartition\_Threshold, 3-16
  - Set Module Network, 3-14
  - Set Port Mode, 3-14, 4-9
  - Set Security Autolearn, 4-8
  - Set Security Autolearn Capture, 4-9
  - Set Security Autolearn Download, 4-12
  - Set Security Autolearn MAC\_Address, 4-11
  - Set Security Port, 4-8
  - Set Security Port MAC Address, 4-11
  - Set Security Port Mode, 4-13
  - Show Port Security, 4-15

- Show Security Autolearn, 4-17
- Show Security Intruder List, 4-19
- Configuration Distance Calculation
  - Sample, 2-9
- Configuration Rules
  - Equivalent Distance, 2-9
  - Fiber Backbone, 2-7
  - General, 2-2, 2-3, 2-5
  - Sample Calculation, 2-9
  - Twisted Pair Backbone, 2-10
- Configuring
  - Autolearn Mask, 4-8
  - Autolearning, 4-9
  - Autopartition Threshold, 3-16
  - Port Redundancy, 3-14
  - Redundant Links, 2-13
  - Security Features, 4-4
  - Security Mode, 4-13
  - Security Module, 3-13

## ***D***

- Defining a MAC Address, 4-11
- Designing a Network, 2-1
- DIP Switch
  - Configuring, 3-5
  - Default Values, 3-7
  - Link Integrity, 3-15
  - Location, 3-5
- Downloading
  - Autolearning Database, 4-12

## ***E***

- Eavesdropping Security
  - Example, 4-5
- Electrical Specifications, A-1
- Electro-Static Discharge
  - Precautionary Procedures, 3-2
- Enabling Ports, 3-14
- Environmental Specifications, A-2
- Ethernet

- Four-Repeater Rule, 2-10

## ***F***

- FCC notice, ii
- Fiber Backbone, 2-7
  - Twisted Pair To-the-Desk, 2-8
- Fiber Equivalent Distance
  - Sample Calculation, 2-9
- Fiber Link Distances, 2-5
- Front Panel
  - Monitoring, 3-18
- Front Panel Indicators
  - Activity LEDs, 3-18, 3-20
  - Status Indicators, 3-18
  - Status LEDs, 3-20

## ***G***

- General Specifications, A-2

## ***H***

- Hot Swap, 3-8

## ***I***

- Installation
  - 50-Pin Cable, 3-12
  - Attaching the 50-Pin Cable, 3-12
  - Hot Swap Capabilities, 3-8
  - Security Module, 3-8
- Intruder List, 4-8
- Intrusion Control
  - Example, 4-6
- Intrusion Detection, 4-5

## ***L***

- LAN Product Equivalent Distances, 2-6
- LED and Network Verification, 3-21
- Link Distances



- Configuration Rules, 1-1
- Link Integrity
  - Configuring, 3-15
  - Description, 3-15
  - DIP Switch Setting, 3-7

## **M**

- Mechanical Specifications, A-2
- MIB, B-4
- MIB Variables, 4-21
- Module Configurations
  - Saving, 3-16
  - Showing, 3-17
- Module Security DIP Switch Setting, 3-15
- Module Status LED
  - Function, 5-3

## **N**

- Network
  - Assignments, 3-14
  - Check Codes, 3-21
  - Configurations, 2-9
  - Designing, 2-1
  - Selection, 3-14
  - Unshielded Twisted Pair, 2-11
- network supplier support, B-2

## **O**

- ONline 10BASE-T Security Module
  - Security Module, 1-1
- ONline Ethernet Management Module, 1-3, 4-18
  - Advanced Version, 4-18
- ONline Management Modules, 3-13, 3-14, 4-1
- ONline System Concentrators, 1-1
  - Hot Swap Capabilities, 3-8
  - TriChannel Architecture, 3-14
- on-line technical services, B-1
- ONline Token Ring Management Module, 1-3

## **P**

- Patch Panels, 2-11
- Port Action on Intrusion
  - Default Setting, 4-8
  - Defining, 4-7
  - Intruder List, 4-8
- Port Configurations
  - Showing, 4-15
- Port Redundancy, 2-13
  - Configuring, 3-14
  - Switchover Conditions, 2-13
- Ports
  - Enabling, 4-8

## **Q**

- Quick Reference Chart, 4-2

## **R**

- Redundant Links, 2-12
- Repeaters, 2-8
- returning products for repair, B-4
- Revert Security Command, 4-14
- RJ-45 Connector Pinouts, A-7

## **S**

- Save Security Command, 4-14
- Saving Module Configurations, 3-16
- Saving Security Configurations, 4-14
- Security Configurations
  - Clearing, 4-19
  - Saving, 4-14
  - Uploading, 4-4
- Security Intruder List
  - Clearing, 4-20
  - Showing, 4-18
- Security Mode
  - Configuring, 4-13
  - DIP Switch Setting, 3-7

- Using With Autolearning, 4-7
- Security Module
  - Activity LEDs, 5-4
  - Configuration Quick Reference Chart, 4-2
  - Configuring, 3-13
  - DIP Switch, 3-5
  - Eavesdropping Security, 4-5
  - Electrical Specifications, A-1
  - Environmental Specifications, A-2
  - Features, 1-1
  - Front Panel, 3-18
  - General Specifications, A-2
  - Hot Swap Capability, 1-2
  - Installing, 3-8
  - Intrusion Detection, 4-5
  - Mechanical Specifications, A-2
  - Module Status LED, 5-3
  - Network Management, 4-1
  - Port Status LEDs, 5-2
  - Procedures for Handling, 3-2
  - Sample Application, 1-2
  - Theory of Operation, 1-2
  - Troubleshooting, 5-1
  - Unpacking Procedures, 3-4
- Security Module LEDs
  - Interpreting, 3-20
- Security Type
  - Default Setting, 4-6
- Set Module Autopartition\_Threshold
  - Command, 3-16
- Set Module Network Command, 3-14
- Set Port Mode Command, 3-14, 4-9
- Set Security Autolearn Capture Command, 4-9
- Set Security Autolearn Download Command, 4-12
- Set Security Autolearn MAC\_Address, 4-11
- Set Security Port Action\_On\_Intrusion
  - Command, 4-8
- Set Security Port MAC Address Command, 4-11
- Set Security Port Mode Command, 4-13

- Setting Security Type, 4-6
- Show Port Security Command, 4-15
- Show Security Autolearn Command, 4-17
- Show Security Intruder List Command, 4-19
- Showing Module Configurations, 3-17, 4-14
- Showing Port Configurations, 4-15
- Showing Security Autolearn, 4-17
- Showing Security Intruder List, 4-18
- SNMP Commands, B-4
- SNMP Variables, 4-21
- Star Topology, 2-3
- Status LEDs
  - Troubleshooting Using, 5-2

## **T**

- Technical Assistance, 5-5
- Technical Support, 5-5
- technical support, B-1
- Theory of Operation, 1-2
- Troubleshooting
  - Security Module, 5-1
  - Technical Assistance, 5-5
  - Using Activity LEDs, 5-4
  - Using Port Status LEDs, 5-2
- Twisted Pair
  - Cables, A-6, A-8
  - Connections, A-6
  - Connectors, A-7, A-8
- Twisted Pair Backbone
  - Configuration Rules, 2-10
  - Twisted Pair To-the-Desk, 2-10
- Twisted Pair Cables, A-8
  - Connecting, A-6
- Twisted Pair Configuration
  - Redundant Links, 2-12
- Twisted Pair Connectors, A-7
- Twisted Pair Wiring
  - Maximum Link Distances, 2-10

## ***U***

- Unpacking Procedures, 3-4
- Unshielded Twisted Pair Cable, 2-8
- Unshielded Twisted Pair Network
  - Sample Configuration, 2-10
- Uploading Security Configurations, 4-4

## ***V***

- VDE compliance, ii
- Verifying
  - Network Assignments, 3-21
- Verifying Module Functionality
  - With LEDs, 3-21

## ***W***

- Wiring Closet, A-8

